

# AS/400 - Remote VPN Clients

P42

ITSO AS/400 e-business University/Technical Forum

Thomas Barlen



# Preface



The first part of this presentation is based on the VPN and L2TP Overview presentation that was produced during an ITSO residency in 1999. The participants in this residency were Thomas Barlen, P. Hey, Y. Kaneko, and L. Kinnunen under the leadership of Marcela Adan.

Additions and modifications were made to focus on remote VPN clients.

# Objectives



## **The purpose of this presentation is to:**

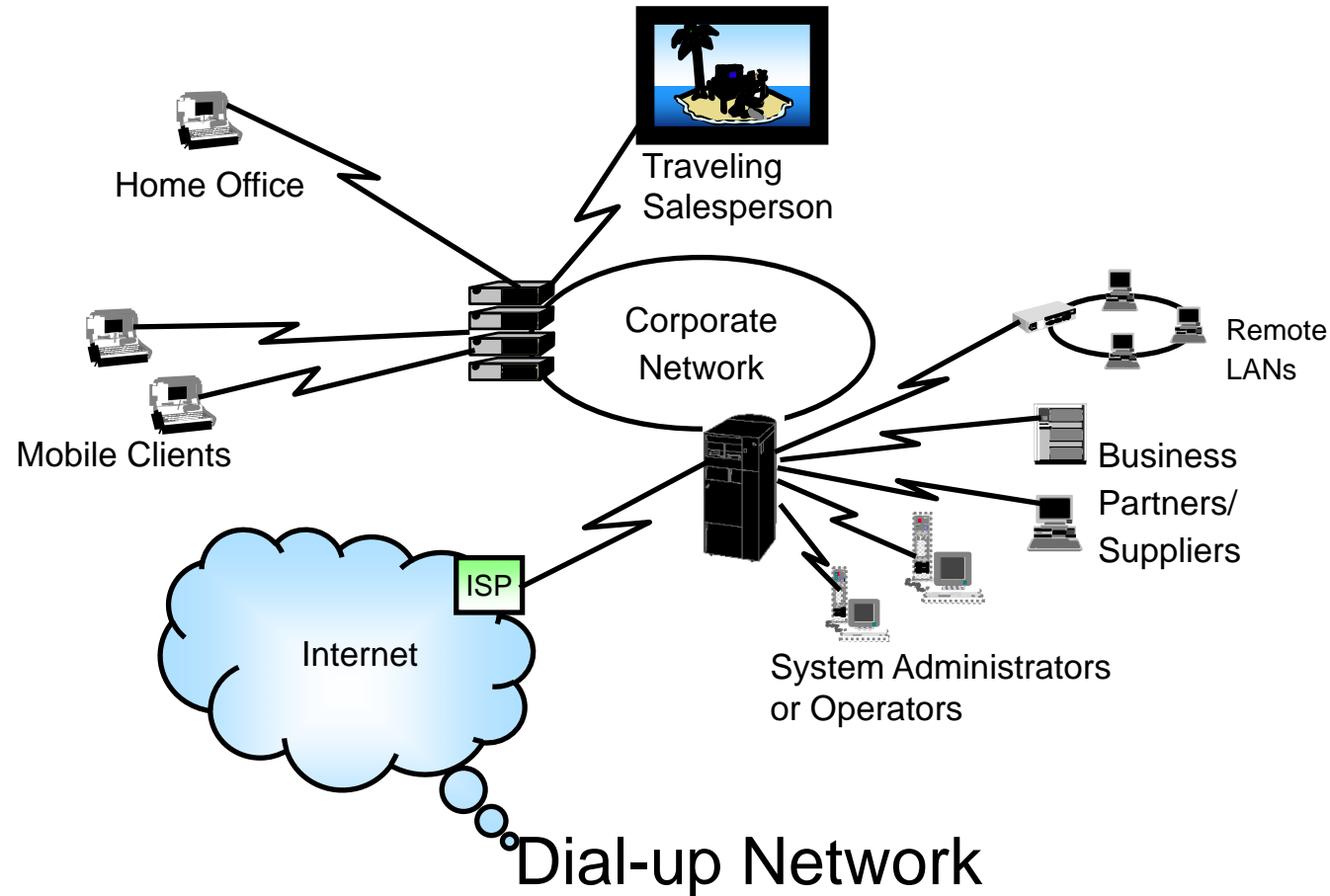
- Provide an overview of VPN technologies and concepts
- Provide a high-level description of the IP Security architecture (IPSec) protocols
- Provide a high-level description of the Layer 2 Tunneling Protocol (L2TP)
- Provide an overview of the remote VPN clients



# Traditional Private Networks



- ✓ High cost to maintain
- ✓ Long-distance calls could be prohibitively expensive



# Notes: Traditional Private Networks

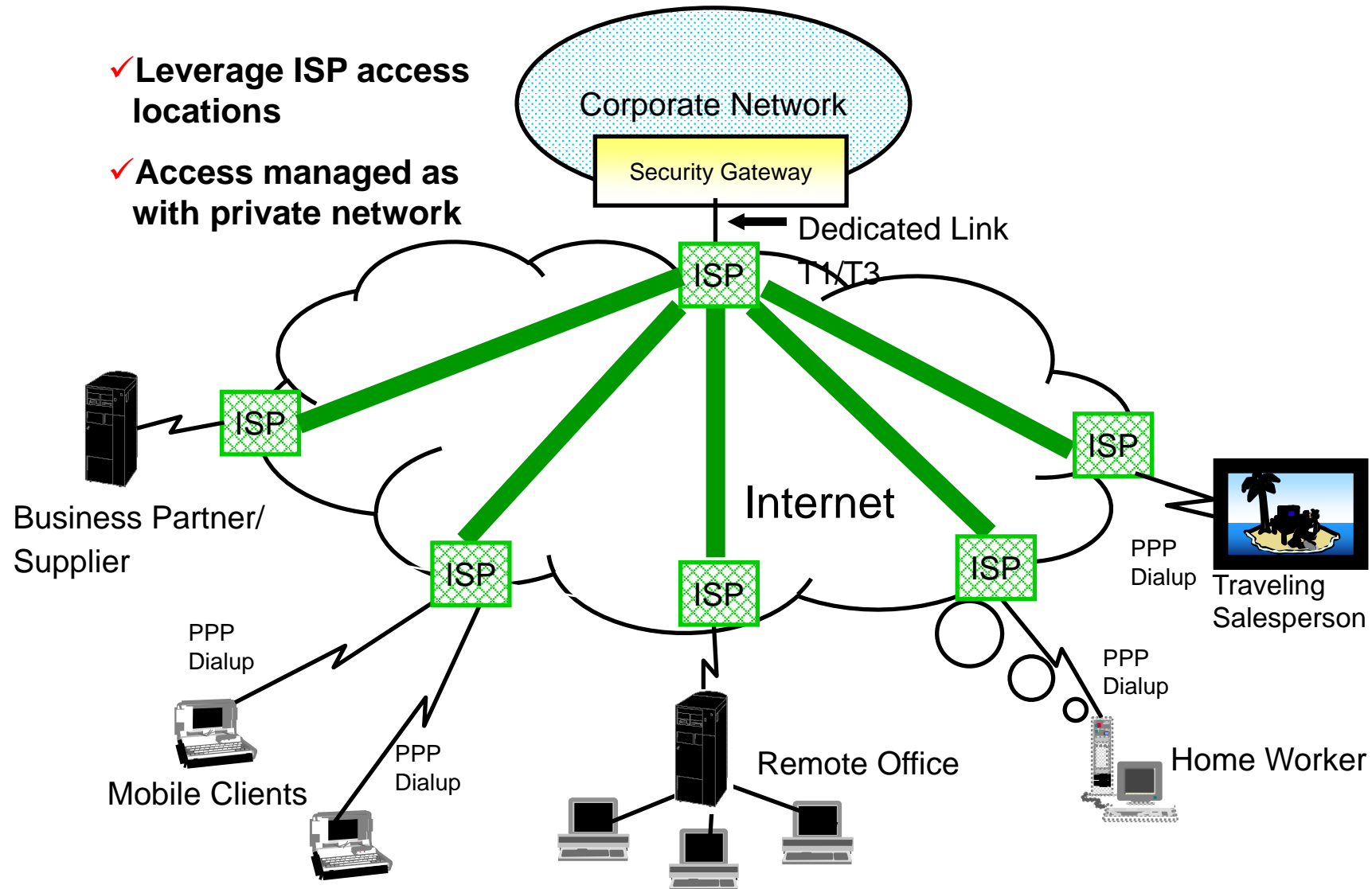


Traditional corporate networks are largely self-contained. All data travels over private facilities. For example, many corporations use dial-up connections, leased lines, or other WAN technologies (such as frame relay) to communicate with their branch offices and remote users. In this closed, tightly controlled environment, the traditional corporate network is considered to be secure, because very little traffic leaves or enters the network.

However, a new business model is emerging. Not only do corporations need to communicate with their branch offices and remote users, but secure *intercompany* communication is also becoming a necessity. This new *extended* corporate network is a collection of physically separated intranets that are connected by the public Internet. The economical, worldwide reach of the Internet also makes it an attractive replacement for the traditional intra-business network.

Ideally, the *modern* private network would retain the desirable characteristics of the traditional private network, while incorporating the cost-effective, global reach of the Internet.

# Modern Private Network



# Notes: Modern Private Network



In a modern private network, your corporation can take advantage of the global reach of the Internet to extend its corporate network to almost anywhere in the world. At the same time, the corporate network maintains control over incoming and outgoing traffic, as in the traditional private network.

There are several advantages to this configuration. One advantage is that your Internet Service Provider (ISP) now provides and maintains the network infrastructure (for example, modem pools, routers, etc.). In a traditional network, the corporation manages the entire network. By off loading some of the administrative requirements to an ISP, your corporation will realize savings in terms of in-house skills and resources. Another advantage is actual monetary savings. When you connect your corporate network to the Internet via an ISP, you will no longer have to pay for expensive leased-lines or long distance phone calls. Your cost will be equal only to your ISP fee (and local phone call, if applicable).



# VPN Customer Value



## Cost Savings

- Eliminates the need for expensive leased lines, long-distance calls, and toll-free telephone numbers
- Estimated 20 to 47% savings in WAN costs and 60 to 80% savings in remote access dial-up costs (Infonetics Research, Inc.)

## Easy Access to Corporate Networks and Resources

- Remote users and remote locations access sensitive information whenever they want and from wherever they are
- Internet access is available worldwide, where other forms of connectivity may be either not available or more expensive



## e-Business

- Focus on gaining competitive advantage
- Strengthen relationships with business partners, suppliers, and distributors

---

© 2000 IBM Corporation  
• Transform the way corporations do business

# Notes: VPN Customer Value



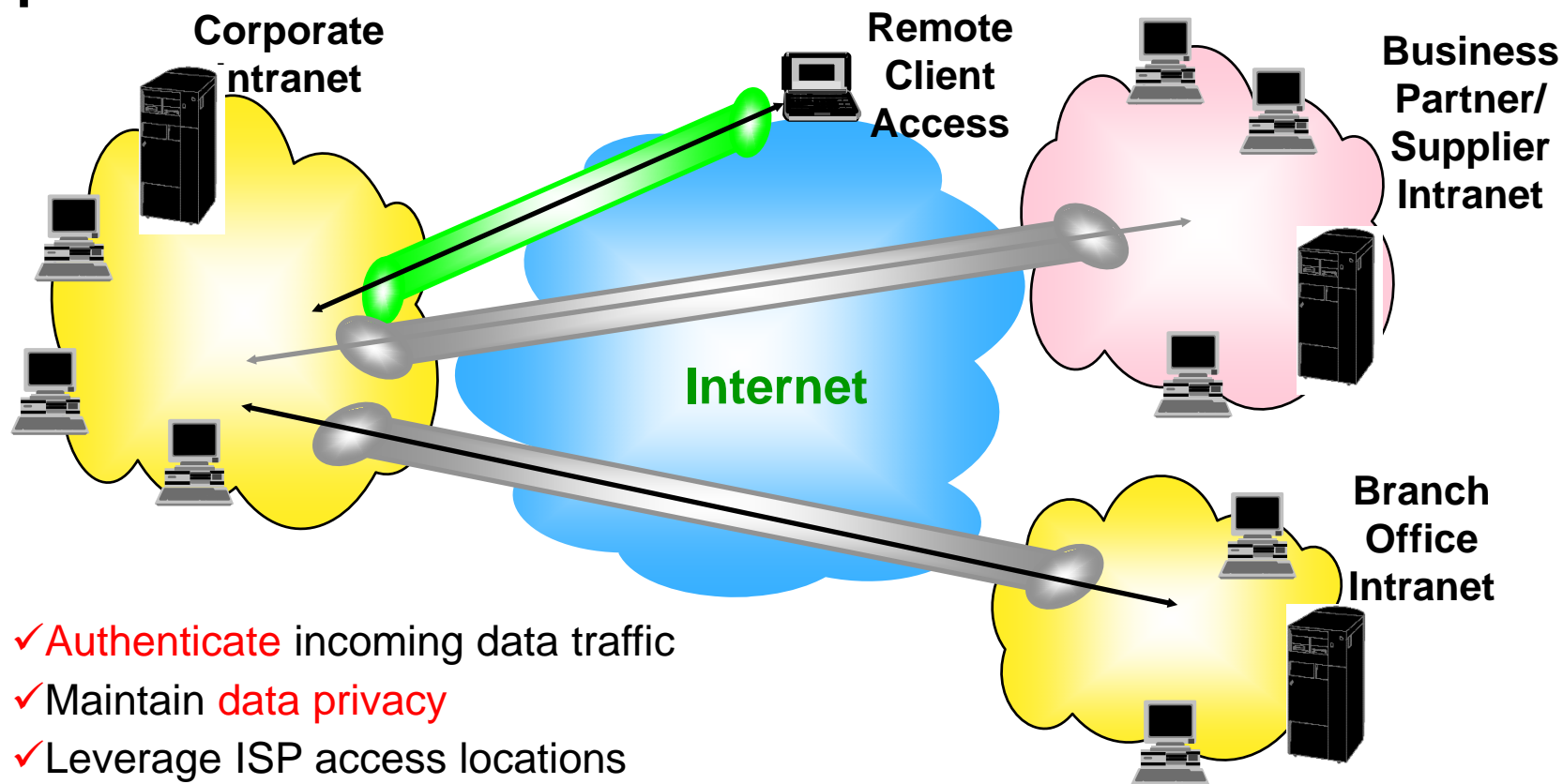
With the explosive growth of the Internet, companies are asking: "How can we best exploit the Internet for our business?" Initially, companies used the Internet to promote their company's image, products, and services by providing World Wide Web access to corporate Web sites. Today, however, the focus has shifted to *e-business*. Companies are leveraging the global reach of the Internet for easy access to key business applications and data that reside in their traditional I/T systems. Companies can now securely and cost-effectively extend the reach of their applications and data across the world through the implementation of secure virtual private network (VPN) solutions.

VPN allows your corporation to make the transition from the traditional private network to the modern private network.

# Virtual Private Networks



**Secure** extension of your company's private intranet across a public network



- ✓ **Authenticate** incoming data traffic
- ✓ Maintain **data privacy**
- ✓ Leverage ISP access locations
- ✓ Manage access as with private network

# Notes: Virtual Private Networking



- ✓ A VPN is an extension of your company's private intranet over the existing framework of a public network, such as the Internet. VPN technologies allow you to control network traffic while providing important security features, such as authentication and data privacy. This is typically achieved by defining a secure *tunnel* through which data flows in an encrypted form, normally indecipherable to eavesdroppers or hackers.
- ✓ As we've discussed, the convenience and security of VPN allows you to communicate with your branch offices, business partners, and remote users at a cost equal only to your Internet Service Provider (ISP) fee.
- ✓ In general, there are three types of VPN implementations that are well-suited to most business needs: Branch office connections, Business partner/supplier connections, and remote user connections.

# VPN Business Opportunities



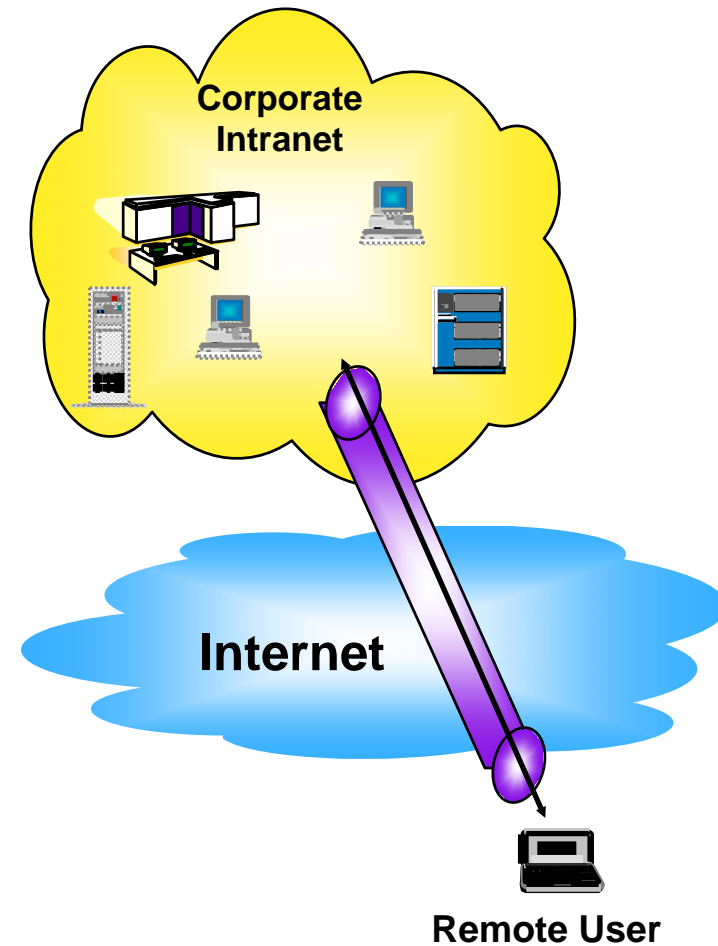
## Remote Access Scenario

### ✓ Problems

High administrative workload cost,  
expensive toll-free numbers or  
long distance costs

### ✓ Solutions

VPNs exploit worldwide ISP reach  
and lower connectivity and  
administrative costs



# Notes: VPN Business Opportunities



Finally, VPN can provide an excellent solution for connecting remote users, either from their homes or while traveling. Rather than installing and managing modem pools and paying long distance call charges (or financing the calls through toll-free numbers), VPN allows users to dial in to a local ISP. The ISP is responsible for providing the modem pool and the Internet provides the "long distance" connection through to your corporate network. Security of remote dial-in access is always a concern; the authentication and optional encryption of VPN provides a safe and reliable solution to this problem.

# VPN Requirements



## Data Origin Authentication

- ✓ Verifies that each datagram was originated by the claimed sender

## Data Integrity

- ✓ Verifies that the contents of the datagram were not changed in transit, either deliberately or due to random errors

## Data confidentiality

- ✓ Conceals the cleartext of a message, typically by using encryption

## Replay Protection

- ✓ Assures that an attacker can not intercept a datagram and play it back at some other time

## Key Management

- ✓ Assures that your VPN policy can be implemented throughout the extended network with little or no manual configuration

## Performance and Availability

- ✓ Assures that the VPN does not hinder your business operations, but rather grows as your business grows. It also assures that your VPN can accommodate future technologies as they become available

## Interoperability

- ✓ Assures that your VPN uses ~~standards-based technologies to maintain~~ interoperability with other VPN vendors

# Notes: VPN Requirements



Implementing a VPN presents your company with many significant challenges. No single entity owns the Internet or sets its policies. Data from many different sources flows through its common backbone infrastructure and within its routers. As the idea of e-business grows, more and more data will flow between companies. As a result, a VPN could potentially present security exposures that were not present in the traditional corporate network model.

There are security exposures everywhere along an end-to-end path: on the dial-up link, in an ISP's access box, on the Internet, in the firewall or router, and even in the corporate intranet. In order to be effective, VPNs must address these basic requirements:

- **Data origin authentication** to verify that each datagram was originated by the claimed sender.
- **Data integrity** to verify that the contents of a datagram were not changed in transit, either deliberately or due to random errors.
- **Data confidentiality** to conceal the cleartext of a message by using encryption.
- **Replay protection** to ensure that an attacker cannot intercept a datagram (containing, for example, an encrypted user ID and password) and play it back at some other time.
- **Key Management** to ensure that your VPN policy can be implemented throughout the extended network with little or no manual configuration. We will discuss key management in more detail later in the presentation.
- **Performance and Availability** to ensure that the VPN does not hinder your business operations, but rather grows as your business grows. Also, ensures that your VPN can accommodate future technologies as they become available. Performance and availability is still a concern in terms of current VPN implementations. However, there are emerging Internet standards that are working to address this requirement.
- **Interoperability** to ensure that your VPN uses standards-based technologies to maintain interoperability with other VPN vendors.

IP Security Architecture (IPSec) provides the first definition of a comprehensive, consistent solution to a majority of these requirements. IPSec can provide end-to-end protection, as well as segment-by-segment protection. Based on the work of the Internet Engineering Task Force (IETF), IBM chose to use IPSec for its IBM SecureWay VPN solutions, including the AS/400 system.



# VPN Protocols

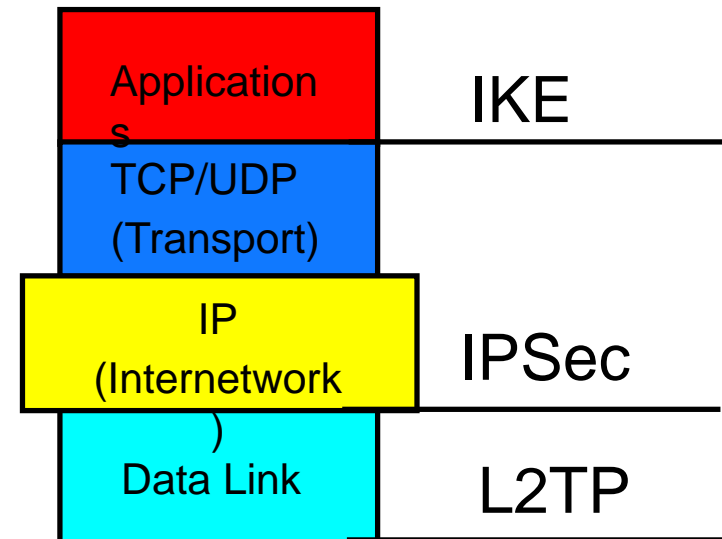


## IP Security Architecture Protocols (IPSec)

- ✓ Open, standards-based, network layer security technology
- ✓ Supports authentication, integrity checking and encryption per packet
- ✓ Provides a key management solution by using the Internet Key Exchange (IKE) protocols (used to be ISAKMP/Oakley)
- ✓ IETF standard in IPv6 (optional in IPv4)
- ✓ Used to secure L2TP tunnels

## Layer 2 Tunneling Protocol (L2TP)

- ✓ Open, standards-based link layer technology
- ✓ Transports multiprotocol data over the Internet
- ✓ Cost-effective (extends PPP connections to the destination network)
- ✓ IETF proposed standard (RFC2661)
- ✓ No inherent security features (use IPSec for security)



# Notes: VPN Protocols



Most VPN offerings can be categorized in several different ways. In our opinion, the most important differentiator is the protocol layer on which the VPN is realized. In the context of this presentation, there are two different approaches to VPN implementation:

- Network layer based solutions that use IPSec
  - Provides blanket protection for all upper-layer application data carried in the payload of an IP datagram. Does not require a user to modify the applications.
- Data link layer based solutions that use L2TP
  - Provides cost-effective remote access by extending the span of a PPP connection. Also provides secure access when used in conjunction with IPSec.

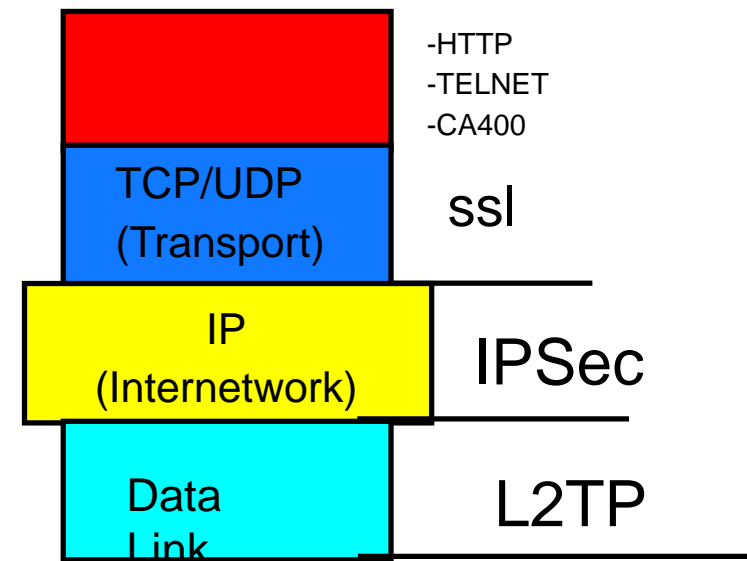
✓There are other methods that operate on upper layers and complement a VPN solution, such as SOCKS, Secure Sockets Layer (SSL), or Secure Multipurpose Internet Mail Extension (S-MIME). Some solutions use only the upper layer protocols to construct a VPN (usually a combination of SOCKS V5 and SSL). While these methods are certainly "players" in terms of VPN implementation, we focus primarily on IPSec and L2TP technologies during this presentation.

# VPN versus SSL Protocols



## SSL

- Requires SSL-enabled server and client applications
- Application to application
- User authentication possible
- Easier to turn on and off
- Allows for more granularity
- Mature technology



## VPN

- Host or gateway must support VPN
- Transparent to application
- Firewall only open for IPsec protocols
- Host authentication
- Leading edge technology

# IPSecurity (IPSec) Protocols



## Authentication Header (AH)

- Provides data origin authentication, data integrity, and replay protection
- Uses hashed message authentication codes (HMAC) based on shared secrets
- Does not encrypt datagram content

## Encapsulating Security Payload (ESP)

- Provides data confidentiality
- Encrypts payload of IP packet by using cryptographic keys
- Optionally provides data origin authentication, data integrity, and replay protection

## Internet Key Exchange (IKE) protocol

- Dynamically generates and refreshes cryptographic keys
- Rekeying occurs while VPN connection is running
- Two phase approach protects keys and data

# Notes: IPSec Protocols



Within the layered communications protocol stack model, the network layer (IP in the case of the TCP/IP stack) is the lowest layer that can provide end-to-end security. Network-layer security protocols provide blanket protection for all upper-layer application data carried in the payload of an IP datagram, without requiring a user to modify the applications.

Network layer security is based on the IP Security Architecture (IPSec) open framework as defined by the IPSec Working Group of the IETF. We call IPSec a framework because it provides a stable, long lasting base for providing network layer security.

IPSec was designed for interoperability. When correctly implemented, it does not affect networks and hosts that do not support it. IPSec is independent of current cryptographic algorithms. However, it supports all of the cryptographic algorithms in use today, and can also accommodate newer, more powerful, algorithms as they become available. The specific implementation of an algorithm for use by an IPSec protocol is often referred to as a *transform*. For example, the DES algorithm used in ESP is called the ESP DES-CBC transform. We will discuss each of the transforms the IPSec protocols support later.

The IETF requires that IPv6 implementations support IPSec, and strongly recommends that IPv4 implementations do as well. IPSec is unique in that it provides base security functions for the Internet, as well as furnishing flexible building blocks from which robust, secure virtual private networks can be constructed.

The IPSec Working Group has concentrated on defining protocols to address the VPN requirements we defined earlier:

- Data Origin Authentication**
- Data Integrity**
- Data confidentiality**
- Replay protection**
- Key Management**

The results are these principal IPSec protocols:

- Authentication Header (AH), which provides data origin authentication, data integrity, and replay protection
- Encapsulating Security Payload (ESP), which provides data confidentiality, data origin authentication, data integrity, and replay protection
- Internet Key Exchange (IKE), which provides a method for automatic key management



# Authentication Header (AH)



## Overview

- ✓ Provides origin authentication for the entire IP datagram
- ✓ Provides data integrity and replay protection
- ✓ IANA assigned IP protocol number 51
- ✓ IETF standard (RFC 2402)
- ✓ Uses hashed message authentication codes (HMAC) based on cryptographic keys
- ✓ Does not encrypt datagram content
- ✓ Two modes: Tunnel and transport

# Notes: Authentication Header (AH)



The AH protocol provides data origin authentication, data integrity, and replay protection. These three distinct functions are often grouped together and referred to as *authentication*. In the simplest terms, AH ensures that your data has not been tampered with en route to its final destination.

Although AH authenticates as much of the IP datagram as possible, the values of certain fields in the IP header cannot be predicted by the receiver. These fields are called mutable and are not protected by AH. However, AH always protects the payload of the IP packet.

In many cases, your data needs only to be authenticated. While the Encapsulating Security Payload (ESP) protocol can perform authentication, AH doesn't affect your system performance as much as the encryption of ESP can. Another advantage of using AH is that AH authenticates the entire datagram. ESP, on the other hand, does not authenticate the leading IP header or any other information that comes before the ESP header. Packets that fail authentication are discarded and are never delivered to upper layers. This greatly reduces the chances of successful denial of service attacks, which aim to block the communication of a host or gateway by flooding it with bogus packets.

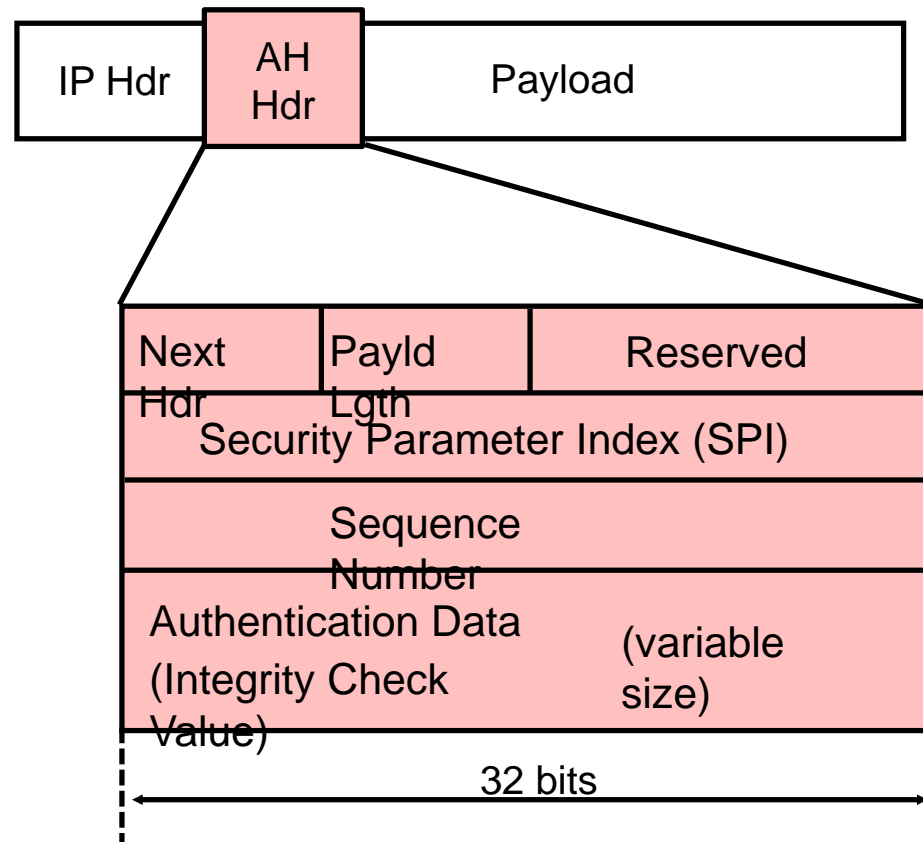
In addition, ESP requires strong cryptographic algorithms in order to be implemented. Strong cryptography is restricted in some countries, while AH is not regulated and can be used freely around the world.

AH is defined in RFC 2402 and is a separate IP protocol (51). For clarification, this means it does *not* use TCP or UDP as an underlying transport protocol.

You can apply AH in two ways: transport mode or tunnel mode.



# AH Packet Format



# Notes: AH Packet Format



This slide shows the position of the AH header in the IP packet and the header fields. The fields are defined as follows:

## Next Header

- The Next Header is an 8-bit field that identifies the type of the next payload after the Authentication Header. The value of this field is chosen from the set of IP protocol numbers defined in the most recent "Assigned Numbers" RFC from the Internet Assigned Numbers Authority (IANA). For example, TCP is assigned protocol number 6, UDP, number 17.

## Payload Length

- This field is 8 bits long and contains the length of the AH header expressed in 32-bit words, minus 2. It does not relate to the payload length of the IP packet as a whole. If default options are used, the value is 4 (three 32-bit fixed words plus three 32-bit words of authentication data minus two.)

## Reserved

- This field is reserved for future use. Its length is 16 bits, and it is set to zero.

## Security Parameter Index (SPI)

- This field is 32 bits in length. We'll discuss SPI in greater detail later in the presentation.

## Sequence Number

- This 32-bit field is a monotonically increasing counter which is used for replay protection. Replay protection is optional. However, this field is mandatory. The sender always includes this field and it is at the discretion of the receiver to process it or not. When a security association is established, the sequence number is set to zero. The first packet transmitted using the SA has a sequence number of 1. Sequence numbers are not allowed to repeat. Thus, the maximum number of IP packets that can be transmitted on any given SA is  $2^{32} - 1$ . After the highest sequence number is used, a new SA and, consequently, a new key is established. Anti-replay is enabled at initiation by default. If, after the SA has been established, the receiver chooses not to use it, the sender is no longer concerned with the value in this field.

-**Note:** Manual key management does not typically use the anti-replay mechanism. In addition, older IPsec implementations, like the one used in the IBM Firewall for AS/400, are based on the original AH specification (RFC 1826), which does not support the concept of sequence numbers.

# Notes: AH Header Format (cont'd)



## Authentication Data

- This is a variable-length field, also called the Integrity Check Value (ICV). The ICV for the packet is calculated by using the algorithm agreed upon when the SA is initialized. The authentication data length is an integral multiple of 32 bits. As its name implies, the receiver uses it to verify the integrity of the incoming packet.
- In theory, any MAC algorithm can be used to calculate the ICV. The specification requires that HMAC-MD5-96 and HMAC-SHA-1-96 are supported. The old RFC 1826 requires Keyed MD5. In practice, Keyed SHA-1 is also used. Implementations usually support two to four algorithms.
- When doing the ICV calculation, the mutable fields are considered to be filled with zero.



# AH Coverage - Transport Mode

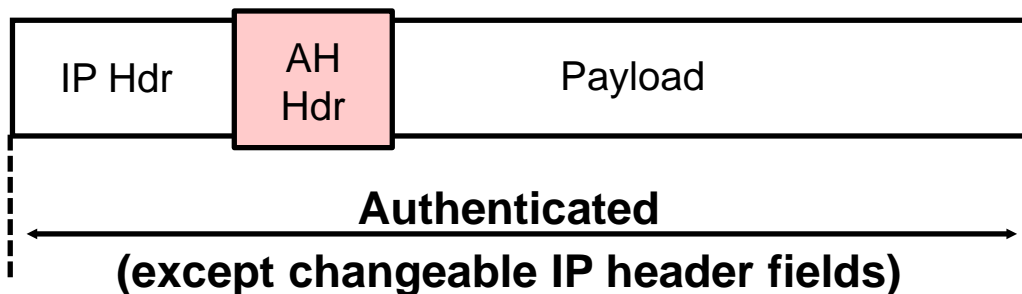


## Transport mode

- ✓ Originating host creates AH header
- ✓ Must be supported by IPSec-enabled **hosts**



Original IP datagram



Datagram with AH header in transport mode

# Notes: AH Coverage - Transport Mode



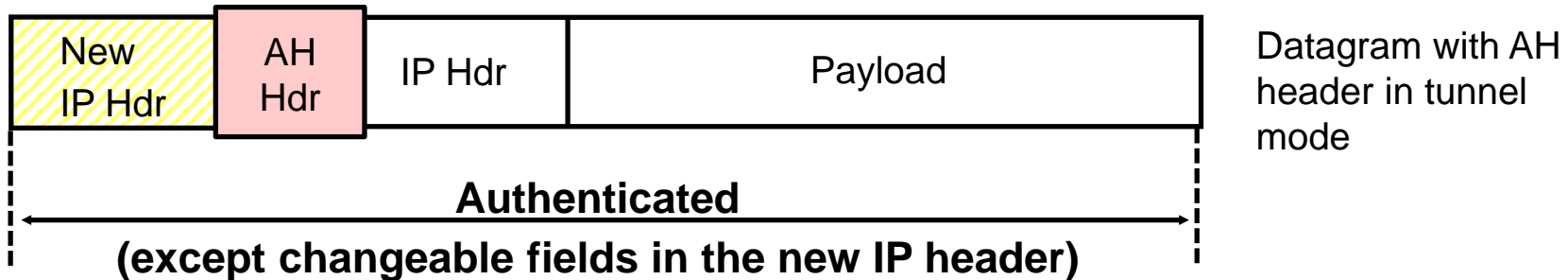
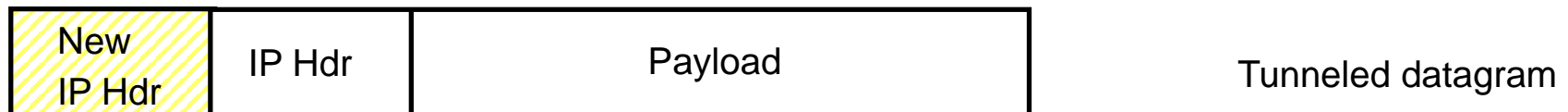
In transport mode, the IP header of the datagram is the outermost IP header, followed by the AH header, and then the payload of the datagram. The entire datagram, except the mutable fields, is authenticated. However, the information contained in the datagram is transported in cleartext form and is, therefore, subject to eavesdropping.

# AH Coverage - Tunnel Mode



## Tunnel mode

- ✓ Intermediate security gateway creates AH header and adds a new IP header
- ✓ Must be supported by IPSec-enabled *hosts* and *gateways*



# Notes: AH Coverage - Tunnel Mode



As this slide illustrates, tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram. The AH header follows the new IP header. The original datagram (both the IP header and the original payload) comes last. AH authenticates the entire datagram, which means that the responding system is able to detect whether changes were made to the datagram in transit.

When either end of a security association is a gateway, you must use tunnel mode. In tunnel mode, the source and destination addresses in the outermost IP header do not need to be the same as those in the original IP header. For example, two security gateways may operate an AH tunnel to authenticate all traffic between the networks they connect. This is a very typical configuration.

One advantage of using tunnel mode is that it totally protects the encapsulated IP datagram. Another significant advantage is that it makes it possible to use *private addresses* in the original IP header. Thus, original datagrams with private source or destination addresses can be routed across a public network if the outer IP header contains public, routable addresses. A tunnel can, therefore, be created across the Internet between two private networks.



# AH Transforms



## Transforms Supported with AH

- ✓ Mandatory Authentication Transforms
  - **HMAC-MD5-96** (RFC 2403)
  - **HMAC-SHA-1-96** (RFC 2404)
- ✓ Optional Authentication Transforms
  - DES-MAC
- ✓ Obsolete Authentication Transforms
  - Keyed-MD5 (RFC 1828)

# Notes: AH Transforms



AH uses algorithms known as hashed message authentication codes (HMAC). The mandatory AH authentication transforms (HMAC-MD5 and HMAC-SHA) both take variable-length input data and a secret key to produce fixed-length output data (called a *hash value*). If the hashes of two messages match, it is likely that the messages are the same. Both MD5 and SHA (Secure Hash Algorithm) encode the message length in their output, but SHA is regarded as more secure because it produces larger hashes.

AS/400 supports HMAC-MD5 and HMAC-SHA authentication algorithms.

# Encapsulating Security Payload (ESP)



## Overview

- ✓ Encrypts the payload of the IP packet using cryptographic keys
  - Next Header field actually identifies the protocol carried in the payload
- ✓ Optional data origin authentication, data integrity, and replay protection
  - Less cryptographic processor power to detect and reject packets whose contents have been changed
  - Reject at IP layer, rather than higher up in the stack
- ✓ IANA assigned IP protocol number 50
- ✓ IETF standard (RFC 2406)

# Notes: ESP

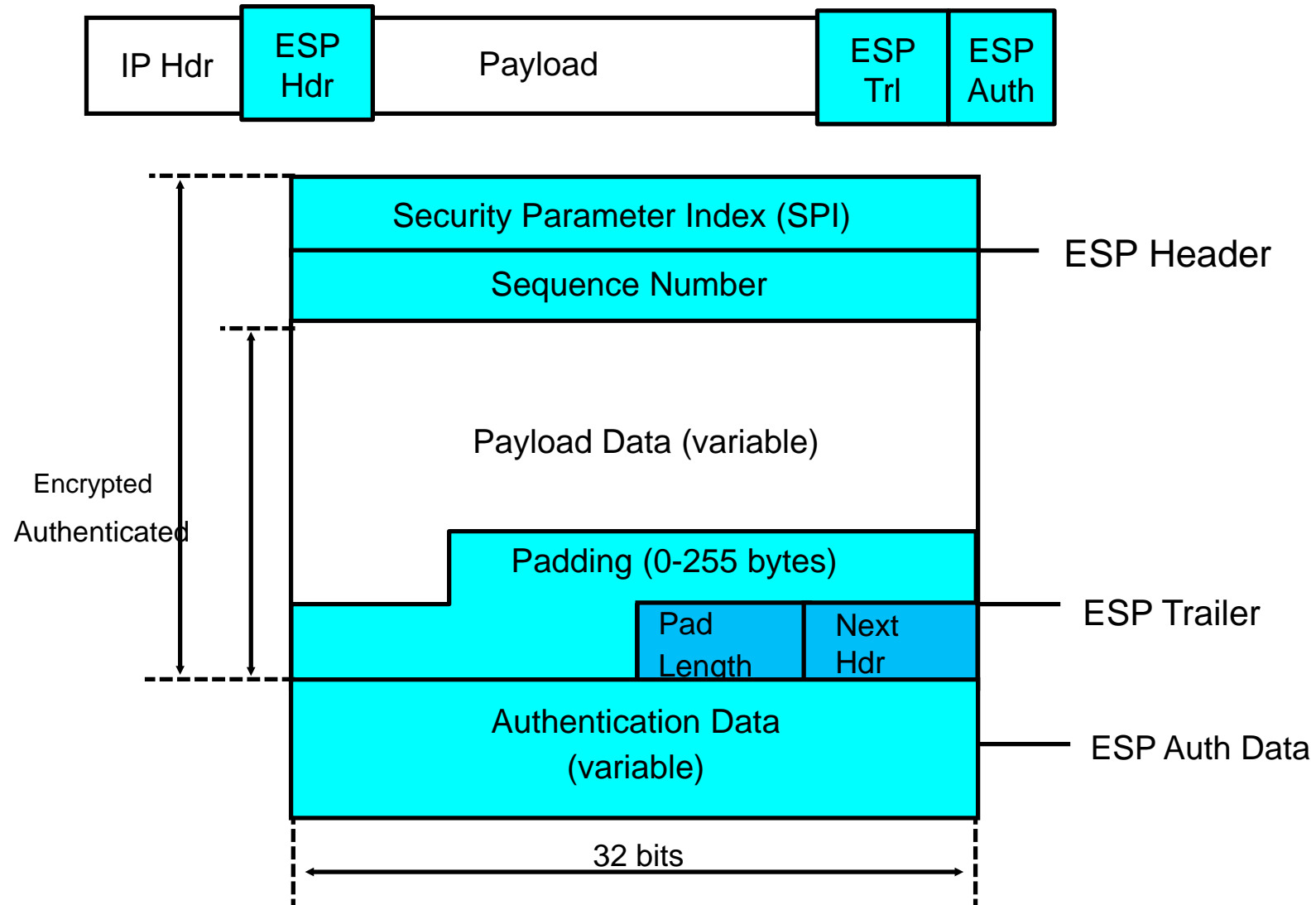


The ESP protocol can provide data confidentiality, and also optionally provide data origin authentication, data integrity checking, and replay protection. The difference between ESP and the Authentication Header (AH) protocol is that ESP has support for encryption, while either protocol provides authentication, integrity checking, and replay protection. Also, AH authenticates the entire datagram, except the mutable fields of the leading IP header. ESP, on the other hand, does not authenticate the leading IP header or any other information that comes before the ESP header. With ESP, both communicating systems use cryptographic keys for encrypting and decrypting the data they exchange.

If you decide to use both encryption and authentication, the responding system first authenticates the packet and then, if the first step was successful, proceeds with decryption. Since decryption is more processor intensive than authentication, this type of configuration reduces processing overhead, as well as reducing your vulnerability to denial of service attacks.

The Internet Assigned Number Authority (IANA) has assigned the protocol number 50 to the ESP protocol.

# ESP Packet Format



# Notes: ESP Header Format



As this slide shows, the format of the ESP packet is more complicated than that of the AH packet. Not only is there an ESP header, but also an ESP trailer and ESP authentication data. The payload is located (encapsulated) between the header and the trailer, hence the name of the protocol. The following fields are part of an ESP packet:

## Security Parameter Index (SPI)

- This field is 32 bits in length. We'll discuss SPI in greater detail later on.

## Sequence Number

- This 32-bit field is the monotonically increasing counter that we described in the AH header format
- **Note:** Manual key management does not typically use the anti-replay mechanism. In addition, older IPsec implementations, like the one used in IBM Firewall for AS/400, are based on the original ESP specification (RFC 1827), which does not support the concept of sequence numbers.

## Payload Data

- The Payload Data field is mandatory. It consists of a variable number of bytes of data described by the Next Header field. This field is encrypted with the cryptographic algorithm agreed upon when the security association was established. If the algorithm requires initialization vectors, these are also included here.
- The ESP specification requires support for the DES algorithm in CBC mode (DES-CBC transform). Often, other encryption algorithms are also supported, such as triple DES and CDMF.

## Padding

- Most encryption algorithms require that the input data be an integral number of blocks. Also, the resulting ciphertext (including the Padding, Pad Length, and Next Header fields) must terminate on a 4-byte boundary, so the Next Header field is right-aligned. This is why this variable length field is included. It can be used to hide the length of the original messages too. However, this could adversely impact the effective bandwidth. Padding is an optional field.
- **Note:** Encryption covers the Payload Data, Padding, Pad Length, and Next Header fields.

## Pad Length

- This 8-bit field contains the number of the preceding padding bytes. It is always present, and the value of 0 indicates no padding.

# Notes: ESP Header Format (cont'd)



## Next Header

- The Next Header is an 8-bit mandatory field that shows the data type carried in the payload, for example an upper-level protocol identifier such as TCP. The values are chosen from the set of IP Protocol Numbers defined by the IANA.

## Authentication Data

- This field is variable in length and contains the ICV calculated for the ESP packet from the SPI to the Next Header field inclusive. The Authentication Data field is optional. It is included only when integrity check and authentication have been selected at SA initialization time.
- The ESP specifications require two authentication algorithms to be supported: HMAC with MD5 and HMAC with SHA-1. Often, the simpler keyed versions are also supported by IPSec implementations.

## Notes:

4 The ICV does not cover the IP header.

5 The original ESP specification in RFC 1827 discusses the concept of authentication within ESP in conjunction with the encryption transform. That is, there is no Authentication Data field and it is left to the encryption transforms to provide authentication.



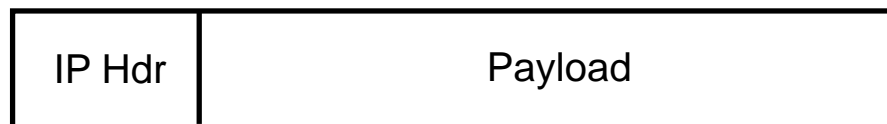


# ESP Coverage - Transport Mode

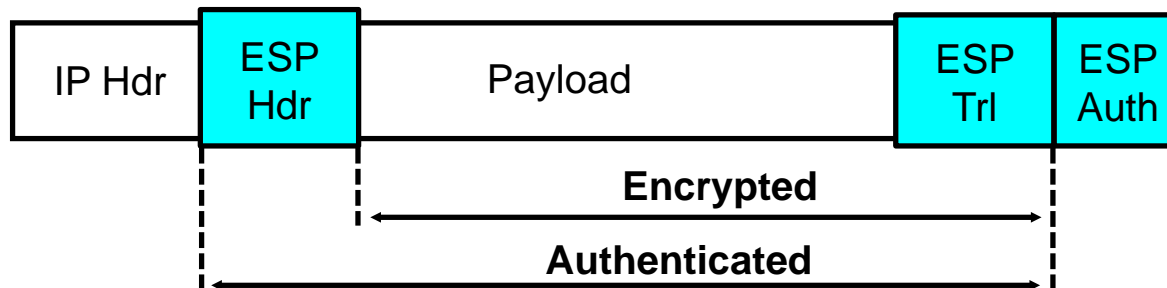


## Transport mode

- ✓ Originating host creates an ESP header
- ✓ Must be supported by IPSec-enabled hosts



Original IP datagram



Datagram with ESP  
in transport mode

# Notes: ESP Coverage - Transp. Mode



In transport mode, the ESP header follows the IP header of the original IP datagram. If the datagram already has an IPSec header, the ESP header goes before it. The ESP trailer and the optional authentication data are appended to the payload of the original datagram.

Transport mode does not authenticate or encrypt the IP header, which could expose your addressing information to potential attackers while the datagram is in transit. Transport mode requires less processing overhead than tunnel mode, but doesn't provide as much security. In most cases, hosts use ESP in transport mode.

# ESP Coverage - Tunnel Mode



## Tunnel mode

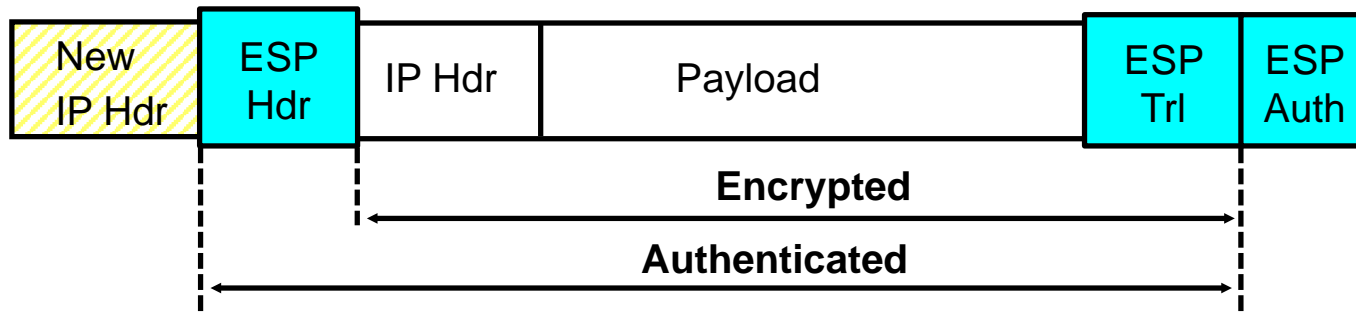
- ✓ Intermediate security gateway creates an ESP header and adds a new IP header
- ✓ Must be supported by IPSec-enabled *hosts* and *gateways*



Original IP datagram



Tunneled datagram



Datagram with ESP in tunnel mode

# Notes: ESP Coverage - Tunnel Mode



- ✓ Tunnel mode creates a new IP header and uses it as the outermost IP header of the datagram, followed by the ESP header and then the original datagram (both the IP header and the original payload). The ESP trailer and the optional authentication data are appended to the payload.
- ✓ If you decide to use both encryption and authentication, ESP completely protects the original datagram because it is now the payload data for the new ESP packet. ESP, however, does not protect the new IP header. Gateways must use ESP in tunnel mode.

# ESP Transforms



## Transforms Supported with ESP

- ✓ Mandatory Encryption Transforms
  - **DES\_CBC** (RFC 2405)
  - **NULL** (RFC 2410)\*
- ✓ Optional Encryption Transforms
  - CAST-128 (RFC 2451)
  - RC5 (RFC 2451)
  - IDEA (RFC 2451)
  - Blowfish (RFC 2451)
  - **3DES** (RFC 2451)
- ✓ Mandatory Authentication Transforms
  - **HMAC-MD5-96** (RFC 2403)
  - **HMAC-SHA-1-96** (RFC 2404)
  - **NULL** (RFC 2410)\*
- ✓ Optional Authentication Transforms

---

▸ DES-MAC

© 2000 IBM Corporation

\*NULL cannot be used for encryption and authentication at the same time

# Notes: ESP Transforms



ESP uses a symmetric key that both communicating parties use to encrypt and decrypt the data they exchange. The sender and the receiver must agree on the key before secure communication takes place between them.

For authentication, ESP uses the same HMAC algorithms that AH uses.

AS/400 VPN supports these authentication and encryption algorithms in V4R4:

- Authentication
  - HMAC-MD5
  - HMAC-SHA
  - None
- Encryption
  - DES-CBC
  - 3DES-CBC
  - RC4
  - NULL

DES is an acronym for Data Encryption Standard. DES produces ciphertexts of the same length as the cleartext and the decryption algorithm is exactly the same as the encryption, the only difference being the subkey schedule. These properties make it very suitable for hardware implementations. Although DES is aging (its origin dates back to the early '70s), after more than 20 years of analysis, the algorithm itself is still considered secure. The most practical attack against it is brute-force: try the decryption with all possible keys and look for a meaningful result. The problem is the key length. Given enough money and time, a brute-force attack against a 56-bit key might be feasible. Therefore, a new mode of DES, called triple-DES or 3DES, has recently gained popularity. With 3DES, the original DES algorithm is applied in three rounds, with two or three different keys. This encryption is thought to be unbreakable for a long time, even with the foreseeable technological advances taken into account.

CBC stands for Cipher Block Chaining mode where the result of the encryption of the previous block is used in the encryption of the current block. Therefore, each *ciphertext* block is dependent not just on the corresponding plaintext block, but on all previous plaintext blocks.

# Key Management Objectives



## Key Generation

- ✓ Cryptography depends on keys
- ✓ SECURE generation of keys is critical
- ✓ Address "first key" problem
  - Initialize keys on links where no security can be assumed
- ✓ Dynamic: As VPN size grows, scalability will become critical to key management
- ✓ Key management protocols

---

- Internet Key Exchange (IKE)

- IBM tunnel

- Manual

# Notes: Key Management



Encryption is the transformation of a cleartext message into an unreadable form in order to hide its meaning. The opposite transformation, which retrieves the original cleartext, is decryption. The mathematical function used for encryption and decryption is the cryptographic algorithm or cipher. The security of a cipher might be based entirely on keeping how it works secret, in which case it is a *restricted* cipher. There are many drawbacks to restricted ciphers. It is very difficult to keep in secret an algorithm used by many people. If it is incorporated into a commercial product, it is only a matter of time and money to get it reverse engineered. For these reasons, the currently used algorithms are keyed, that is, encryption and decryption make use of a parameter, the key. The key can be chosen from a set of possible values, called the keyspace. The keyspace usually is huge, the bigger the better. The security of these algorithms rely entirely on the key, not on their internal secrets. In fact, the algorithms themselves are public and are extensively analyzed for possible weaknesses.

DES is an example of a *symmetric or secret-key algorithm*. Symmetric algorithms are keyed algorithms where the decryption key is the same as the encryption key (contrast this with the more processor intensive *asymmetric or public-key algorithms* where different *public* and *private* keys are used). Symmetric algorithms are the conventional cryptographic algorithms, where the sender and the receiver must agree on the key before any secured communication can take place between them.

The problem is, how do you securely and reliably communicate the key before you have an encrypted link to send it over? And how do you have an encrypted link without a key? You could pass it verbally over the phone, but this is potentially subject to eavesdropping and may be unreliable for complex hexadecimal keys. Consider also that you will want to change keys on a regular basis to reduce the time available and hence the chance of them being broken.

A manual connection or manual tunnel requires that keys are generated and configured manually. All IPSec implementations should support this, effectively as a lowest common denominator.

Some proprietary mechanisms exist for automatically exchanging keys, for example IBM IP Security Protocol (IPSP) or *IBM Tunnel* as supported by IBM Firewall for AS/400 at V4R3. But these are, by definition, proprietary and nonstandard.

The IETF has proposed a standard that allows for dynamic key management/generation called the Internet Key Exchange (IKE) protocols.



# Internet Key Exchange (IKE)



## Overview

- ✓ Key generation and identity authentication
- ✓ Automatic key refresh
- ✓ Solves the "first key" problem
- ✓ Based on ISAKMP framework and Oakley key distribution protocol
- ✓ IETF standard (RFCs 2408-09, 2411-12)
- ✓ Built-in protection
  - Prevents *Denial of Service* attacks
  - Prevents *Man-in-the-Middle* attacks
  - Provides *Perfect Forward Secrecy*
- ✓ Must support IKE over UDP, port 500
- ✓ Must use strong authentication
  - Pre-shared keys
  - Digital signatures (DDS and RSA)
  - Public key encryption (RSA and revised RSA)
- ✓ Two-phase approach

# Notes: IKE



Internet Key Exchange (IKE) framework, previously referred to as ISAKMP/Oakley, is a proposed IETF standard which supports the automated negotiation of Security Associations, and the automated generation and refresh of cryptographic keys.

Generating your keys securely is the most important factor in establishing a secure and private connection. If your keys are compromised, your authentication and encryption efforts, no matter how strong, become worthless. The ability to perform this function with little or no manual configuration will become an ever more critical element as your VPN grows in size.

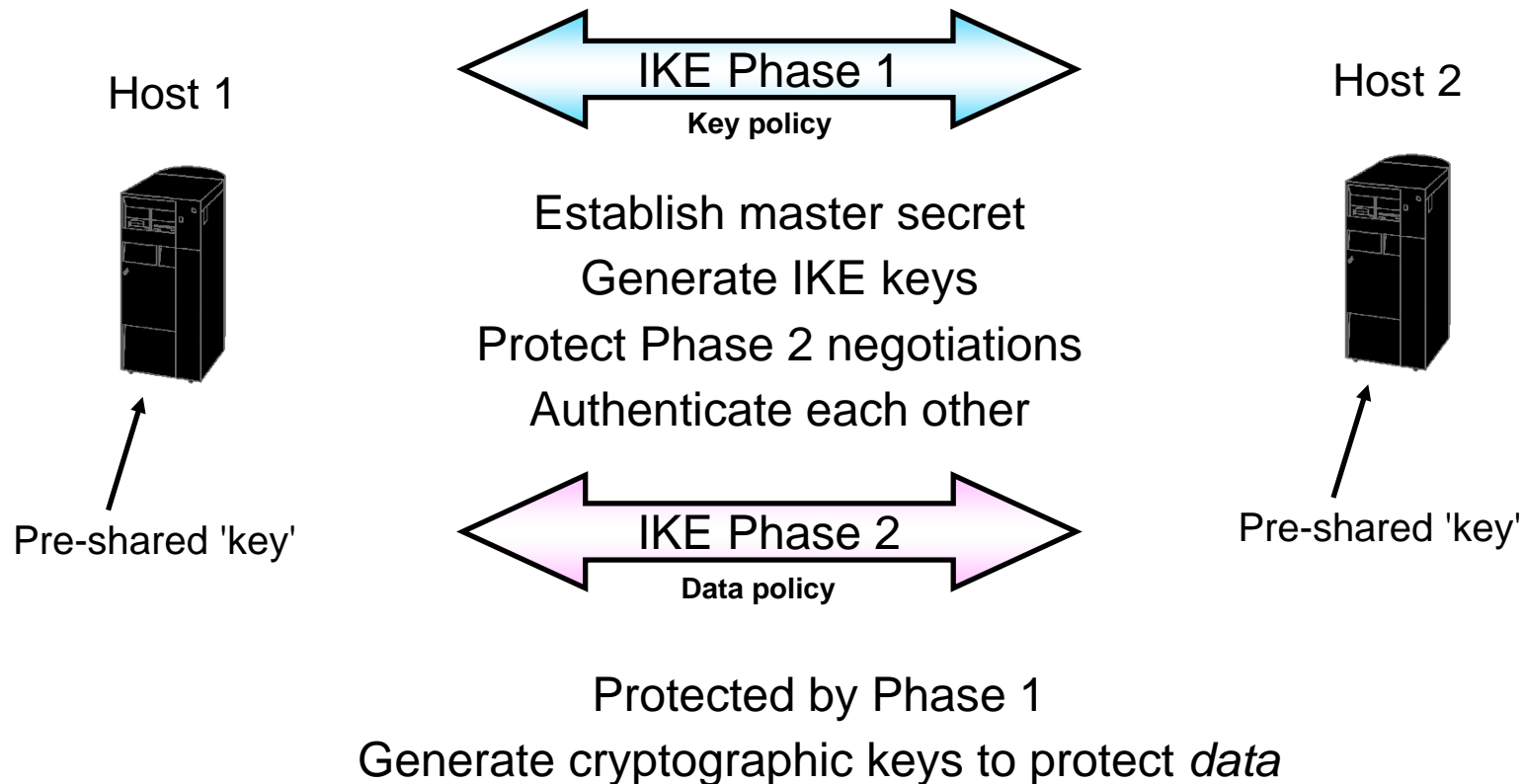
IKE requires that all information exchanges be both encrypted and authenticated. That way, no one can eavesdrop on your keying material, and your keying material is generated only among authenticated parties. IKE procedures deal with initializing the keys, so they must be capable of running over links where no security can be assumed to exist. Therefore, the IKE protocols use the most complex and processor-intensive operations in the IPSec protocol suite.

In addition, the IKE methods have been designed with the explicit goals of providing protection against several well-known exposures:

- Denial of Service: Identifies and rejects invalid messages without running processor-intensive cryptographic operations.
- Man-in-the-Middle: Prevents common attacks, such as deletion of messages, modification of messages, reflecting messages back to the sender, replaying of old messages, and redirection of messages to unintended recipients.
- Perfect Forward Secrecy: Compromised keys provide no useful clues for breaking any other key, whether it occurred before or after the compromised key. Each refreshed key is derived without dependence on past keys.

✓IKE uses the UDP protocol with source and destination port number of 500.

# The Two Phases of IKE



Keys are derived, never  
transmitted

# Notes: The Two Phases of IKE



IKE uses two distinct phases in its implementation. Phase 1 establishes a shared master secret from which subsequent cryptographic keys are derived in order to protect user data traffic. This is true even if no security protection yet exists between the two endpoints.

Various authentication methods can be used to authenticate Phase 1 negotiations, as well as to establish the keys that protect the IKE messages that flow during the subsequent Phase 2 negotiations. These include pre-shared keys, digital signatures, public key encryption and revised public key encryption. At V4R4, AS/400 VPN only supports pre-shared keys. The advantage of pre-shared keys is their simplicity. The disadvantage is that a shared secret must be distributed out-of-band prior to IKE negotiations.

Pre-shared key is perhaps a misnomer. In fact, a predefined character string is agreed upon and entered manually on both endpoint VPN key servers, but this is not really the key. The actual keys are derived, starting with a *Diffie-Hellman key exchange*. Briefly, using the Diffie-Hellman algorithm, a large random number is generated on each key server and used to exponentiate an agreed integer value. The resulting exponents are exchanged and each key server then exponentiates the received exponent again using its random number. Both key servers now have the same result (the original integer exponentiated by both random numbers) which can be used as an initial shared secret key. The security of the exchange is based on the fact that it is extremely difficult to inverse the exponentiation performed by the two parties (the random numbers used are never transmitted). This shared secret key is then applied to the pre-shared key (and some other exchanged values called *Nonces*) to derive a string of bits called keying material from which all other authentication and cryptographic keys are generated.

**It is important to understand that keys themselves are never entered or communicated between servers, but derived using agreed upon inputs and algorithms by each of the key servers.**

# Notes: Continued...



Phase 2 negotiates the keys and encryption or authentication algorithms that will protect the actual application data exchanges. Remember, up to this point, no application data has actually been sent. Phase 1 protects the Phase 2 IKE messages. Once Phase 2 negotiations are complete, your VPN establishes a secure, dynamic connection over your network and between the endpoints that you defined for your connection. All data that flows across the VPN is delivered with the degree of security and efficiency that was agreed upon by the key servers during the Phase 1 and Phase 2 negotiation processes.

In Phase 1, the cryptographic operations are the most processor-intensive but need only be done infrequently, and a single Phase 1 exchange can be used to support multiple subsequent Phase 2 exchanges. In general, Phase 1 negotiations are implemented once a day or perhaps once a week, while Phase 2 negotiations are refreshed as often as every couple of minutes. Higher refresh rates increase your data security, but decrease system performance. Use short key lifetimes to protect your most sensitive data.

**Note:** AS/400 VPN terminology refers to Phase 1 as the *key policy*, and to Phase 2 as the *data policy*.

# Notes: Continued...



For your information....

Here is an expanded example of a Diffie-Hellman exchange:

- Remember, Diffie-Hellman is used to derive a shared secret. It is based on the difficulty of finding discrete logarithms in finite fields of size  $m$ .
- Two parties (say, Alice and Bob) share two public values, a modulus  $m$  and an integer  $g$ ;  $m$  should be a large prime number.
  - Alice generates a large prime number  $a$  and computes  $X = (g^a) \bmod m$ .
  - Bob generates a large prime number  $b$  and computes  $Y = (g^b) \bmod m$ .
  - Alice sends  $X$  to Bob.
  - Bob computes  $K1 = (X^b) \bmod m$  and sends  $Y$  to Alice.
  - Alice computes  $K2 = (Y^a) \bmod m$ .
  - $K1$  and  $K2$  are equal to  $(g^{ab}) \bmod m$ ; this is the shared secret.

Below is an expansion of how keying material is generated during Phase 1:

- SKEYID is the keying material from which all further keys are derived to protect ISAKMP and protocol SAs. It is generated differently depending upon the authentication method used.
- For pre-shared keys:
  - $SKEYID = \text{prf}(\text{Pre-shared Key}, NA, NB)$ 
    - $\text{prf}$  identifies the pseudo-random function agreed to in the first exchange.
    - $NA, NB$  are nonces exchanged during Phase 1 negotiations (*nonce* is a fancy name for a value that is considered to be random according to some very strict mathematical guidelines).

# IKE Modes



Two IKE Phase 1 modes are supported...

## 'Main' mode

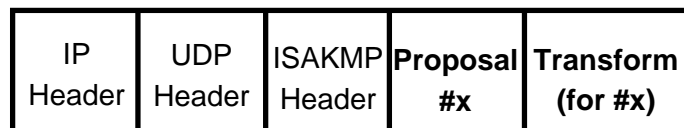
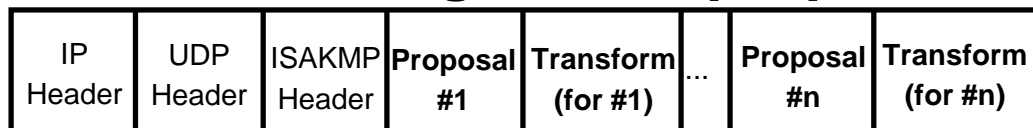
- Also known as 'identity protection' mode
- Encrypts identities during Phase 1 negotiations

## 'Aggressive' mode



- Faster
- Doesn't encrypt identities
- Used for most dial-up connections (pre-shared key)

**Both modes negotiate a proposal for transforms to be used..**



# Notes: IKE Modes



IKE supports two modes, *main* or *identity protection* mode and *aggressive* mode. Main mode encrypts the identities of the key servers. In the simplest case, these are their IP addresses, but IKE also supports the use of *permanent* identifiers, such as a name or e-mail address. Aggressive mode is faster than main mode because it uses a three message exchange rather than six, but identifiers flow in cleartext. **Note:** The IP header of the UDP datagrams always contains unencrypted IP addresses. Otherwise, routing would not be possible. In some cases, however, it may be that the key servers use different IP addresses than those used externally.

In Phase 1, the initiator offers one proposal for the transforms (at least one) to use and, in Phase 2, the initiator can offer multiple proposals (with a minimum of 1) for the transforms to use. Each proposal can contain multiple transforms. You will remember that transforms are the authentication and encryption algorithms to be used.

- The responder looks through its own list of proposals and selects the first that matches. The sequence in which proposals are checked is controlled by the initiator. Matches must be exact, for example 3DES will not match DES. There is one exception: if key expiration times are different, the lower time will be accepted.



# OS/400 V4R4 VPN Support



- Integrated in the Operating System (5769-SS1)
- Requires IBM Crypto Access Provider (5769-AC2, or AC3)
- VPN GUI Requires Client Access Express (5769-XE1)



<http://www.icsa.net>

"**Choose Your Weapons Wisely.** The goal for the ICSA certification is to contribute significantly to making the digital world a safer place. The ICSA certification does this by applying its risk reduction framework to develop the criteria by which industry-wide categories of products are tested. Those products that become 'ICSA Certified' have met a definable quantitative level of risk reduction against a known set of threats."

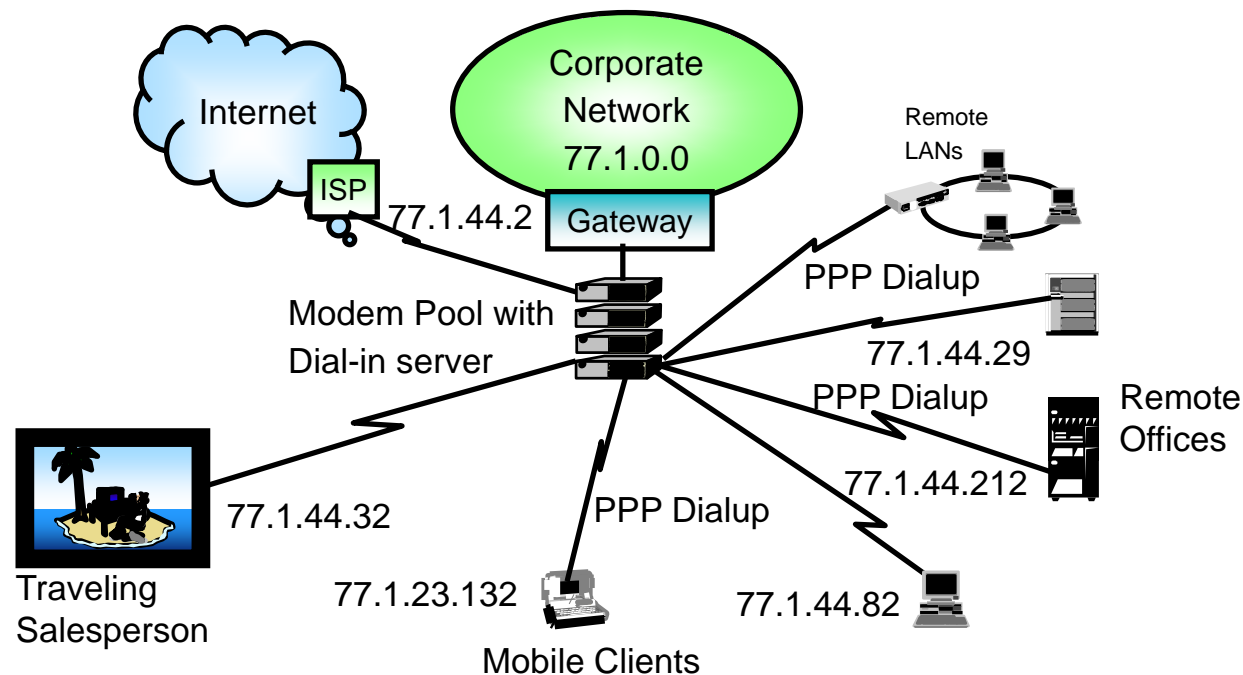


# **L2TP Overview**

# Traditional Dial-Up Network



- ✓ Clients appear as locally connected to the corporate network
- ✓ Clients are connected to a Remote Access Server to the corporate network



## Dial-up Network

# Notes: Traditional Dial-Up Network



In traditional dial-up networks, the client (for example, a business partner, a salesperson, or mobile workers) dial into the corporate network over the public telephone network. The typical dial-in entry point of the corporate network consists of a modem pool with an associated dial-in access server.

Most of the time, the connections are long-distance and, therefore, expensive. Another issue that contributes to the high cost is maintenance. As the number of remote users grows, the modem pool, access server ports, and number of telephone lines, must be extended.

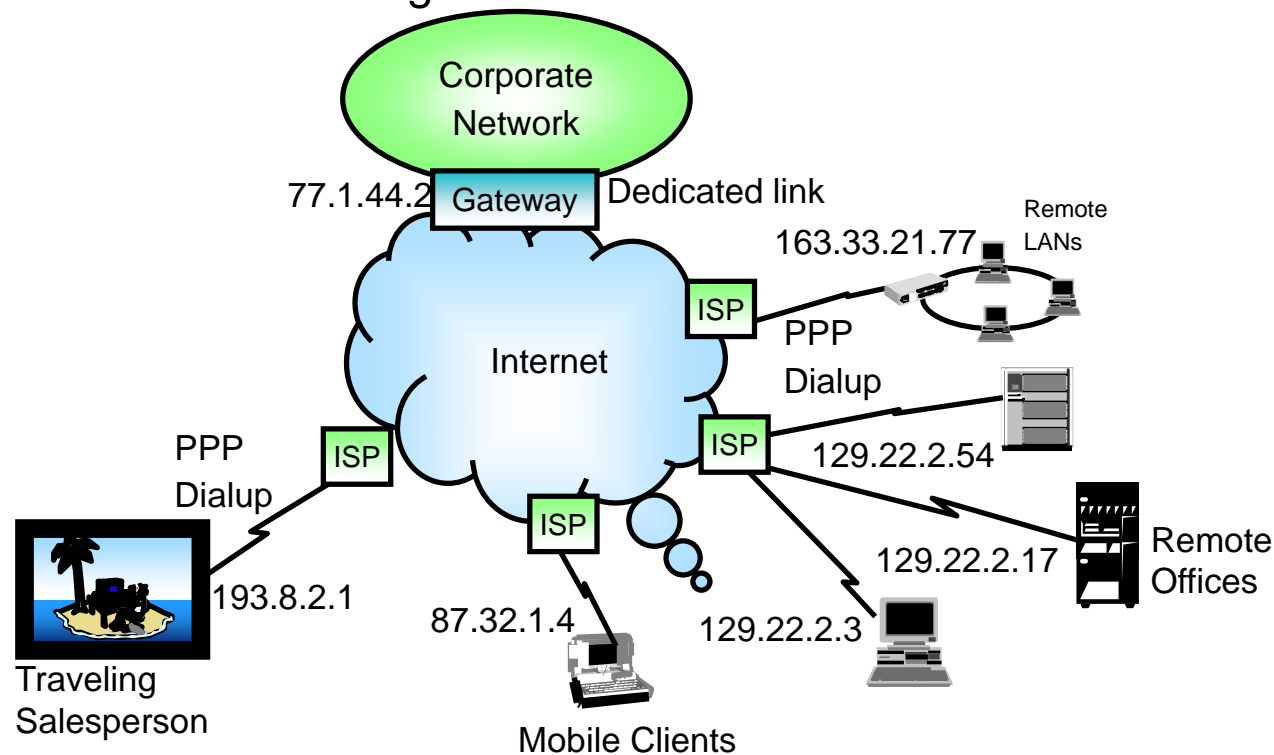
Since the remote users dial into the corporate network, they can use any service within the corporate network. They get, for example, an IP address of the corporate network they are assigned to. Therefore, they appear as locally connected.

This method of connecting a remote user to the corporate network met the requirements in the past. But today, where the business needs changed, you may also want to connect business partners or supply companies to your corporate network. Some remote clients need access to the entire corporate network, and other clients just need access to a particular subnet or system in the corporate network. At this point, traditional dial-up networks reach their limits.

# Modern Dial-Up Network



- ✓ Generally, all connections are to a local ISP, not directly to the corporate network
- ✓ Only Headquarters require dedicated links with security gateway
- ✓ Share dedicated link with remote access as well as general Internet traffic
- ✓ Clients get IP addresses assigned from the ISP rather than from the corporate network



## Dial-up Network

# Notes: Modern Dial-Up Network



Modern dial-up networks exploit the Internet to connect remote clients to the corporate network. On the corporate side there is just a dedicated link required to the Internet. This link can be used for remote access as well as the traditional Internet traffic, such as e-mail, and World Wide Web access.

The remote clients dial into the nearest Internet Service Provider (ISP) point of presence (PoP). These calls are usually local calls and, therefore, save an enormous amount of money compared to long-distance calls.

The modern dial-up network as depicted in this chart also opens many new issues:

- Is the Internet as a carrier secure?
- What happens to the IP addresses of the remote client? In the traditional dial-up network, the addresses are local to the corporate network. In the modern dial-up network they are usually dynamically assigned by the ISP.
- How can home workers be restricted to corporate traffic only? The company may want to control the Internet access itself, for example, the employee should enter the Internet through the company's Internet gateway and not directly.

All these issues require a solution that gives the remote client transparent access to the corporate network and, of course, the data should also be protected.

L2TP, in combination with VPN, is the right answer. It provides transparent access for the remote clients to the corporate network. Basically, L2TP extends your local IP address space to a remote client over the intervening Internet. The data can be protected by VPN in different ways.

# L2TP Characteristics



## ✓ Remote client appears as locally connected to the corporate network

- ▶ The remote client appears as directly connected to the corporate network, as seen in traditional dial-up networks
- ▶ Has the same access to the corporate network as locally attached clients
- ▶ The same security gateway rules, as defined for local clients, apply to the remote clients
- ▶ Remote client access can be restricted to the corporate network only
- ▶ Eliminates the need for opening firewalls for remote clients

## ✓ Used to tunnel PPP traffic

- ▶ The basic idea of L2TP is to extend the corporate network over an intervening network (the Internet, for example) to the remote client
- ▶ The user data traffic is encapsulated in a virtual PPP link and then tunneled into a L2TP tunnel

## ✓ L2TP, in combination with IPSec, provides a secure connection over the Internet

# Notes: L2TP Characteristics



The traditional method by which companies provide connectivity to their networks for mobile and remote users is to install and manage large modem pools and remote-access servers. This approach is costly, not only in dollars, but also in time and other resources. Issues, such as size of the modem pool and the geographic locations of the points-of-presence, demand ongoing attention. To circumvent these costs, companies look at outsourcing their remote access services to Internet service providers. Users connecting to the Internet through ISPs can access corporate services from anywhere in the world.

However, the traditional dial-up network service on the Internet is for registered (also known as global routable addresses) IP addresses only. Therefore, a new class of dial-up application services, which allows multiple protocols and unregistered IP addresses, is also desired on the Internet. Examples of this class of network services include support for privately addressed IP, IPX, SNA, and NetBios dial-up via PPP across existing Internet infrastructure. PPP is a protocol (RFC1661) which supports multiprotocol dial-up, in addition to user authentication and network layer address resolution. Layer Two Tunneling Protocol (L2TP) is a protocol which manages the tunneling of the link layer (for example, sync HDLC, async HDLC) of PPP. Using L2TP tunnels, it is possible to divorce the location of the initial dial-up server from the location at which the dial-up protocol connection is terminated and access to the network provided.

Virtual PPP technology extends the normal PPP session created between the client and the remote-access server to a home gateway on the Internet. The home gateway terminates the PPP session and performs all the functions of a remote-access server, including user authentication and protocol negotiation. Virtual PPP dial-up allows many separate and autonomous protocol domains to share common access infrastructure, including modems, Access Servers, and routers. The support of these multiprotocol virtual dial-up services (note that PPP on the AS/400 system only supports the IP protocol) is of significant benefit to end users, enterprises, and Internet Service providers, because it allows the sharing of very large investments in access and core infrastructure and allows local calls to be used. It also allows existing investments in non-IP protocol applications to be supported in a secure manner while still leveraging the access infrastructure of the Internet. L2TP dial-up tunnels are implemented in one of two models, depending on client connectivity.

In the modern dial-up network without L2TP, the user accepts that the IP address may be allocated dynamically from a pool of ISP addresses. This model often means that the remote user has little or no access to their corporate network's resources, due to firewalls and other security policies applied by the corporate network to accesses from external IP addresses. For the Virtual PPP link, the L2TP network server can exist behind the corporate firewall, allocating addresses which are internal. In this case, the dial-in user appears to be locally connected at the L2TP network server.



# Notes: L2TP Characteristics (cont'd)



The L2TP tunnel is viewed as a virtual PPP connection. From the traditional dial-up network point of view, the remote client also used a PPP dial-up link into the corporate network. It got a local IP address and was directly connected to the corporate network. L2TP offers this functionality over the Internet. The traditional PPP link is now tunneled into a L2TP tunnel and therefore called a virtual PPP connection. This virtual PPP connection is tunneled through the Internet to a destination, such as the corporate network.

Due to the fact that the remote client appears as locally connected to the corporate network, it can access all the services within the corporate network. This can be compared to the traditional dial-up network, where the remote client directly dialed into the corporate network. In this case, the remote client also got a corporate IP address assigned. The same security rules for local clients also apply for remote clients. For example, if a local client is only allowed to use a proxy server to connect to the Internet, this restriction would also apply to the remote client.

L2TP as a protocol combines the benefits of the Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft and the Layer 2 Forwarding protocol (L2F) developed by Cisco Systems. In addition, new functions were added, for example, authentication through the IPSec protocol.

L2TP became a proposed IETF standard (RFC2661).

L2TP supports two tunnel modes, the voluntary and the compulsory tunnel. The major difference between these two tunnel modes is the tunnel endpoint. On the voluntary tunnel, the tunnel ends at the remote client and the compulsory tunnel ends at the ISP. The tunnel modes are explained in detail later in this presentation.

# Notes: L2TP Characteristics (cont'd)



L2TP provides the authentication methods of PPP. These are PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).

The CHAP is used to periodically verify the identity of the peer using a three-way handshake. This is done upon initial link establishment, and may be repeated any time after the link has been established. CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges. This authentication method depends upon a "secret" known only to the authenticator and that peer. The secret is not sent over the link.

The Password Authentication Protocol (PAP) provides a simple method for the peer to establish its identity using a two-way handshake. This is done only upon initial link establishment. After the Link Establishment phase is complete, an ID/Password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated. PAP is not a strong authentication method. Passwords are sent over the link "in the clear", and there is no protection from playback or repeated trial and error attacks. The peer is in control of the frequency and timing of the attempts. Any implementations which include a stronger authentication method (such as CHAP) must offer to negotiate that method prior to PAP. This authentication method is most appropriately used where a plain text password must be available to simulate a login at a remote host. In such a use, this method provides a similar level of security to the usual user login at the remote host.

When IPSec protocols are used to protect the L2TP tunnel, more robust authentication transforms are in place compared to the relatively less sophisticated PPP authentication methods.

The Network Control Protocol (NCP) is used to negotiate and assign the IP addresses used for the virtual PPP link.

# Basic L2TP Components



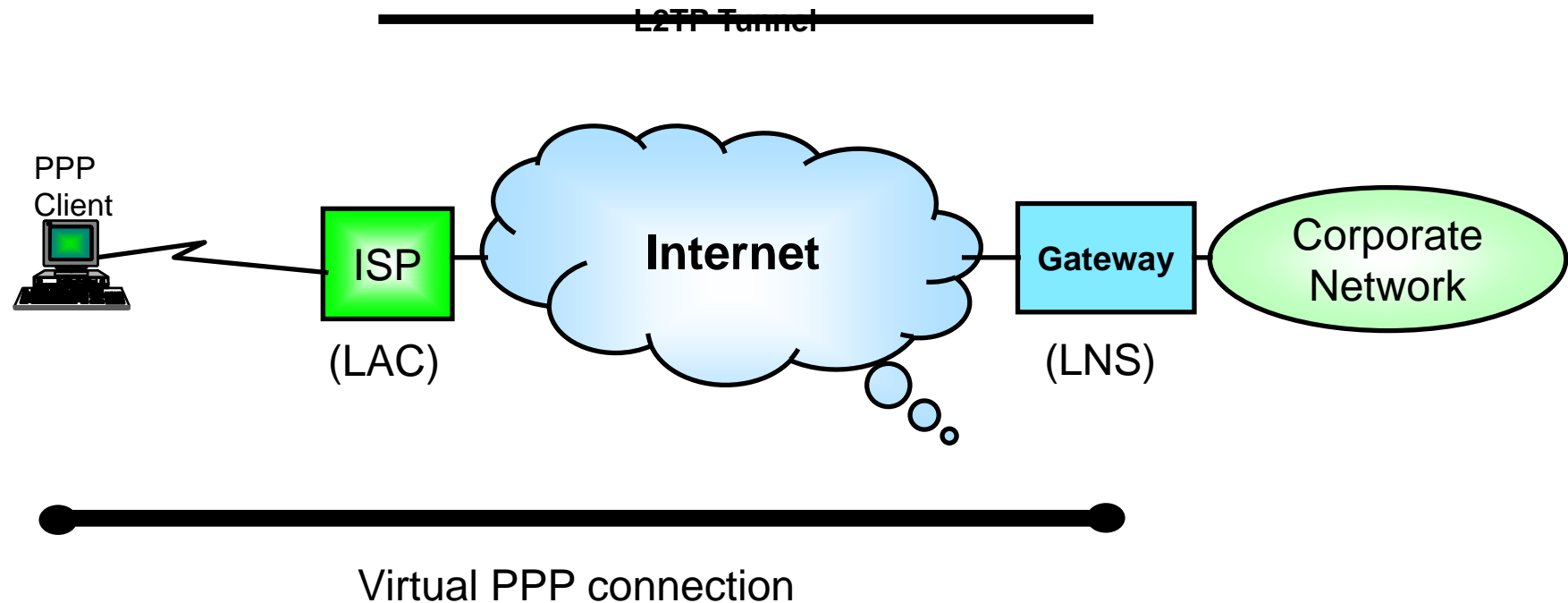
## ✓ L2TP Access Concentrator (LAC)

- ▶ Is the peer to the L2TP Network Server (LNS)
- ▶ Is located at the remote site (ISP or remote client)
- ▶ LAC is the initiator of incoming calls and the receiver of outgoing calls

## ✓ L2TP Network Server (LNS)

- ▶ Is the peer to the LAC
- ▶ Is located at the corporate network site
- ▶ LNS is the initiator of outgoing calls and the receiver of incoming calls.
- ▶ The LNS is the logical termination point of a virtual PPP session that is being tunneled from the remote system by the LAC.

# L2TP Compulsory Tunnel



LAC = L2TP Access Concentrator  
LNS = L2TP Network Server

# L2TP Compulsory Tunnel Concept



- ✓ **Requires no L2TP function on the PPP client**
- ✓ **ISP has to support the LAC**
- ✓ **ISP initiates the L2TP tunnel**
- ✓ **No global routable IP address is assigned to the PPP client**
  - Only one session possible to home gateway
  - Client has no direct access to the Internet (intrusion protection)
- ✓ **The L2TP tunnel is transparent to the client**
- ✓ **L2TP tunnel is between ISP and corporate network gateway**

# Notes: L2TP Compulsory Tunnel



The L2TP compulsory tunnel does not require any configuration on the remote client. The ISP has to provide the L2TP Access Concentrator (LAC) function. The corporate network side has to provide the necessary network and access information to the ISP.

In compulsory tunneling, a tunnel is created without any action from the user and without allowing the user any choice. As a result, the user sends PPP packets to the ISP Network Access Server (NAS)/LAC, which encapsulates them in L2TP and tunnels them to the LNS. The ISP establishes the L2TP tunnel.

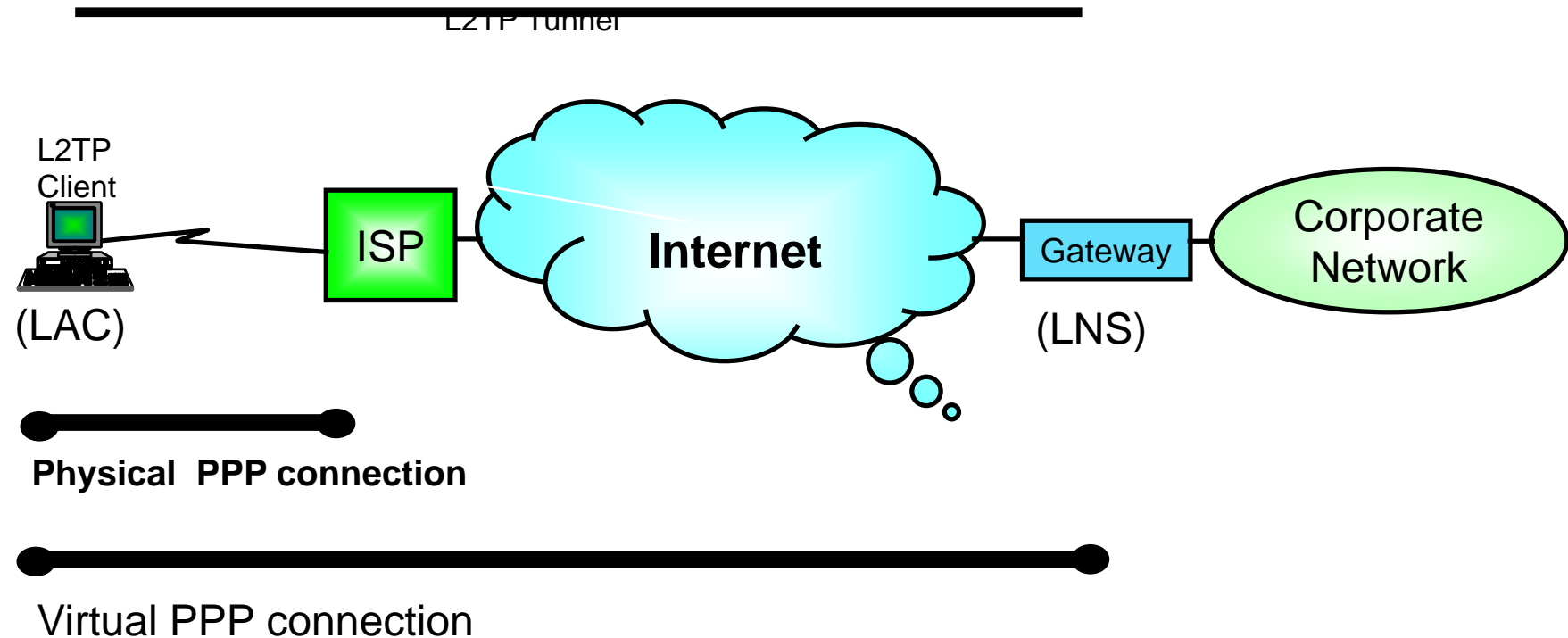
A user dials an ISP and establishes a PPP session with the network access service (NAS), which answers the incoming call and forms one end of the virtual PPP tunnel, and the client. The NAS tells the home gateway (the other end of the virtual PPP tunnel) that an L2TP session has been requested. The NAS then forwards the client's user name and password. If the user is valid, the NAS and the home gateway establish the tunnel and assign a session ID that specifically identifies the user to its tunnel. Once the user has been authenticated and the tunnel is established, the client and the home gateway negotiate the PPP session, setting up protocols and allocating network addresses to the client. In this model the tunneling process is transparent to the user. The user sends PPP packets to the NAS, which encapsulates them in L2TP and tunnels them to the home gateway. When the client establishes the PPP link to the ISP, the ISP assigns an IP address to the client based on the information stored in the LAC database. This IP address belongs to the corporate network at the LNS side. Therefore, the address is not a global routable address. The client has no direct access to the Internet. Instead, the client appears as locally connected to the corporate network and underlies all access and security rules applied to the corporate network.

The client has only a single connection to the remote tunnel endpoint. It cannot have connections to multiple LNS.

Since the client has no global routable IP address, it is protected against intrusion from the Internet

The compulsory tunnel also supports a dial-out function. In this case, the LNS gateway sends a request to the ISP's LAC containing dial-out information. The ISP then establishes a dial-up PPP connection to a remote client.

# L2TP Voluntary Tunnel



LNS = L2TP Network Server  
LAC = L2TP Access  
Concentrator

# L2TP Voluntary Tunnel Concept



## ✓ **L2TP Client (LAC) Initiates Tunnel to LNS**

- Requires the L2TP LAC function on the client
- Additional configuration required on the client

## ✓ **Requires no collaboration by ISP**

- Tunnel is transparent to ISP and Internet access method
- Client can use any ISP PoP

## ✓ **Global routable IP address is assigned to the client**

- Multiple sessions possible
- Client has direct access to Internet
- Client may have multiple IP addresses assigned
  - By ISP for initial connection (physical PPP link)
  - By home gateway for IP/PPP/L2TP connection



# Notes: Voluntary Tunnel Concept



In voluntary tunneling, a tunnel is created by the user, typically by using a L2TP tunneling client. As a result, the user sends L2TP packets to the NAS which forwards them on to the LNS. In voluntary tunneling, the NAS does not need to support L2TP, and the LAC resides on the remote client.

Additional configuration is required on the remote client side.

In this tunnel mode, an L2TP enabled client establishes a PPP session to an ISP. The ISP assigns a global routable IP address to the client. The client then launches an L2TP session directly to its corporate gateway without any involvement from the ISP. The client must first establish an L2TP tunnel with its corporate gateway using a global IP address. Once the L2TP tunnel has been established, the client and the corporate gateway must negotiate the virtual PPP session, setting up protocols and allocating network addresses for communications with hosts on the corporate network. In this model the client implementation is more complex, but it offers more flexibility, enabling multiple access and eliminating the need to establish secure tunnels with ISPs and corporate gateways. In the voluntary tunnel mode, the combined role of the client (user and LAC on the same system) is transparent to the corporate gateway.

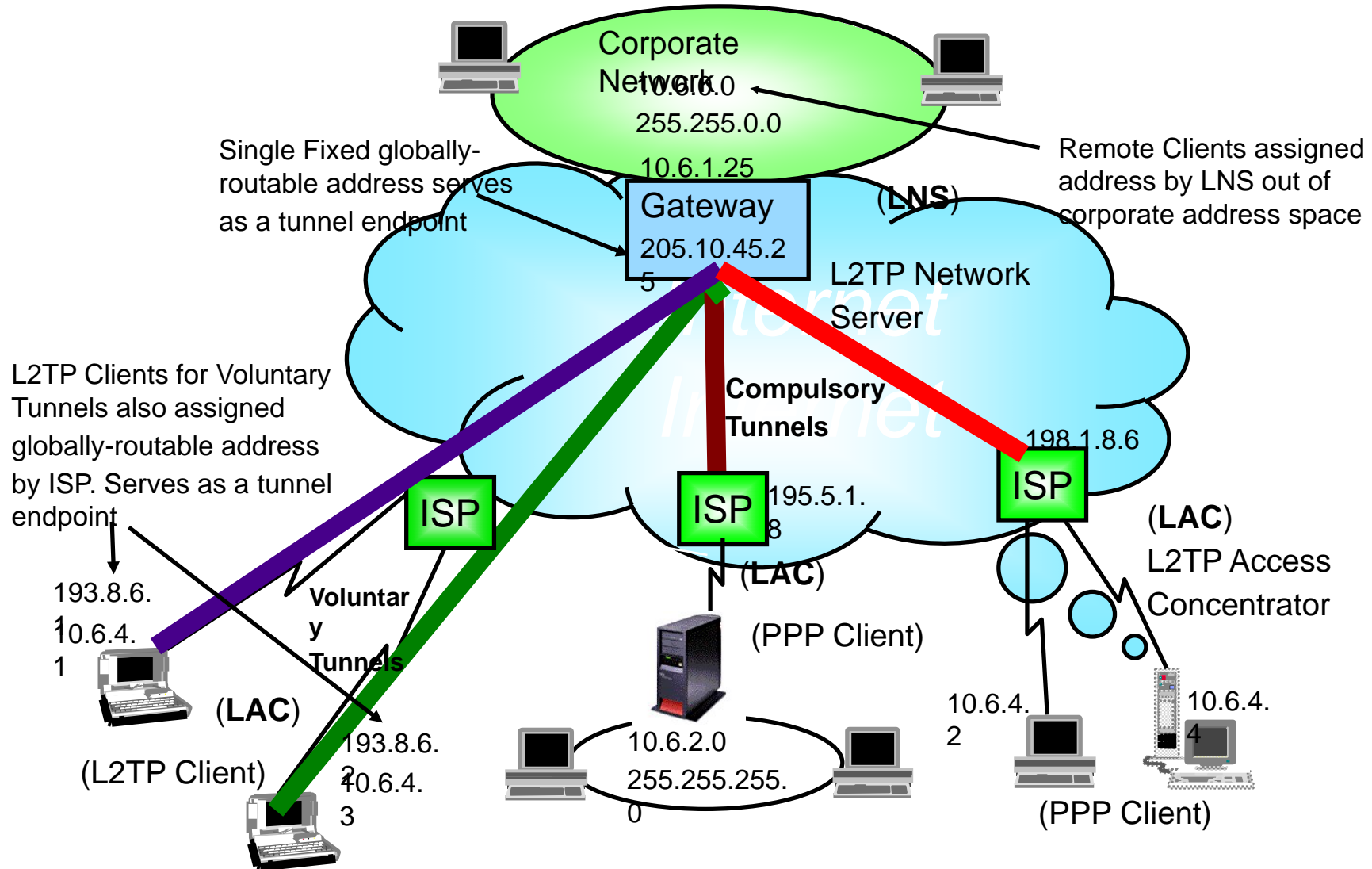
The client can have multiple tunnels established to different LNSs. The client has more than one IP address assigned to it. For example, the global routable IP address and the virtual PPP endpoint address.

Since the client has a global routable address, it has direct access to the Internet. Due to the corporate network IP address (virtual PPP endpoint), the client also appears as locally connected to the corporate network.

Today's choice for an L2TP implementation is the voluntary tunnel, since it is independent of the ISP support. A remote client can use any ISP Point of Presence (PoP) to connect to the corporate network through an L2TP voluntary tunnel.



# L2TP IP Address Management



# Notes: L2TP IP Address Management



The LNS always needs a global routable IP address assigned, whether a voluntary or a compulsory tunnel is used. This address is a fixed address.

In the case of a compulsory tunnel, the remote client gets only an IP address of the corporate network assigned. This might be a registered IP address of the corporate network or a private IP address (for example, 10.21.1.1). The IP address is assigned from the LNS gateway on the corporate site. The AS/400 system at the branch office is assigned a private IP address that cannot be reached from the Internet. In this case, there is little need for a firewall in the branch office. The employees at the branch can access Internet services like other users in the corporate network through the corporate firewall.

If the remote client is the LAC, it is assigned a global routable IP address and a corporate network address. The global routable IP address is the L2TP tunnel endpoint on the client site. The corporate network address is the virtual PPP endpoint address. Both IP addresses may be assigned dynamically, where the global routable address is assigned by the ISP and the virtual PPP endpoint address is assigned by the LNS gateway on the corporate site.

Using the globally routable IP address, users can access Internet services directly. However, they are exposed to attacks since the client is assigned an IP address that can be reached from the Internet.

# L2TP Support on the AS/400 System



✓ **Included in OS/400 V4R4**

✓ **AS/400 supports LNS**

- Virtual PPP line terminator
- Voluntary and compulsory tunnel mode

✓ **AS/400 supports LAC**

- Virtual PPP line initiator
- Voluntary tunnel client only (no LAC ISP support)

## L2TP Support on the AS/400 (cont'd)



### ✓ L2TP tunnel protection with IPSec

### ✓ IPSec protocols AH or ESP can be used to protect the L2TP tunnel

- ▶ Provides Authentication or Encryption for the user data, including the PPP and L2TP header within the Internet
- ▶ Protects the entire connection from the remote client to the LNS gateway in voluntary tunnel mode through the intervening network
- ▶ In compulsory tunnel mode, the PPP header between the remote client and the ISP is not protected by IPSec
- ▶ Protection ends at the LNS gateway on the corporate site

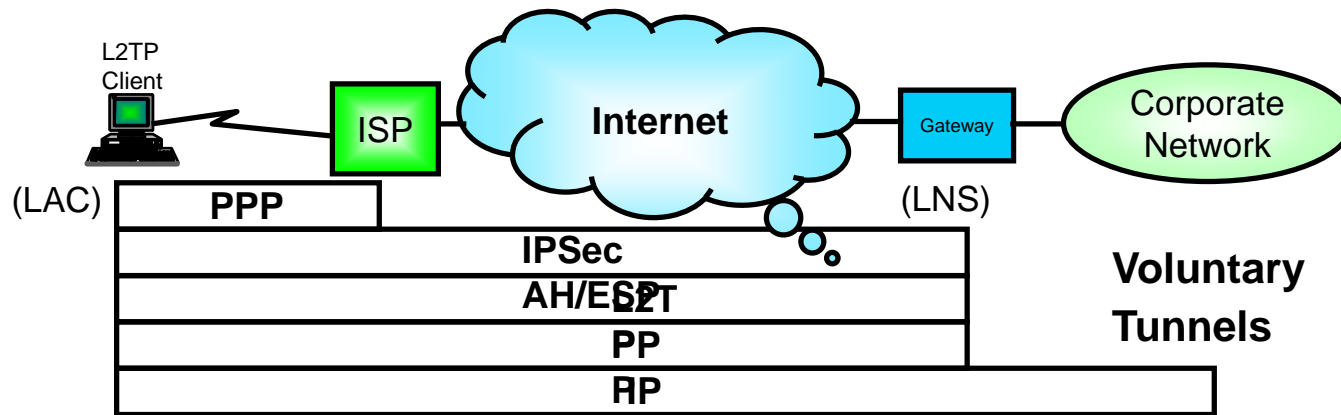
### ✓ End-to-end protection for IPSec enabled destinations

- ▶ Provide end-to-end protection for IPSec enabled hosts in the corporate network and the remote client

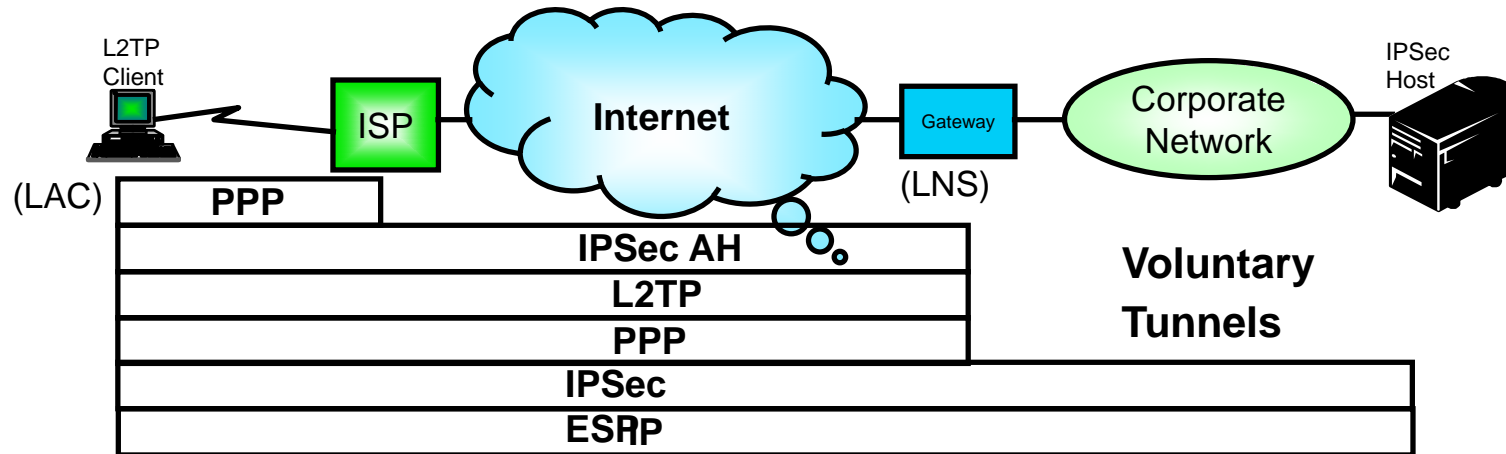
# L2TP Support on the AS/400 (cont'd)



## Non-IPSec-enabled destinations:



## IPSec-enabled destinations:



# Notes: L2TP Security with IPSec



The IPSec protocols Authentication Header (AH) or Encapsulated Security Payload (ESP) can be used to protect a L2TP tunnel. There are slight differences in the protection level, depending on the tunnel mode used. In the voluntary tunnel mode, all the traffic, including the L2TP and virtual PPP header, is protected by IPSec. In the compulsory mode, all traffic is protected, except the PPP header between the remote client and the ISP.

If the destination host in the corporate network is also IPSec enabled, the client can establish a second VPN connection to the destination host. This provides end-to-end security.



# Virtual PPP Profile



## ✓ Selected through Line Connection Type in PPP profile

- ▶ Virtual Line (L2TP)
  - Extends the PPP leased and switched connection types
- ▶ Two mode types available for virtual lines
  - Initiator
    - Used if the AS/400 system is the L2TP client (LAC)
    - Voluntary Tunnel
  - Terminator (network server)
    - Used if the AS/400 system is the L2TP Network Server (LNS)
    - Voluntary and Compulsory Tunnel
    - Used as the tunnel endpoint for remote L2TP clients

# Notes: Virtual PPP Profile



The virtual PPP link that is tunneled through an L2TP tunnel requires a new PPP connection type. This connection type is a virtual PPP connection. In V4R4, there is a new Line Connection Type value available in the PPP connection profile. The new value is Virtual line (L2TP). Once this connection type is selected, two mode types appear in the pull-down list. These values are:

- Initiator

- The L2TP initiator profile needs to be configured on the L2TP client site. The AS/400 system can only be an L2TP client (LAC). It does not support the LAC function needed for the compulsory tunnel. The peer configuration of an Initiator profile has to be an L2TP Terminator profile.

- Terminator (network server)

- An L2TP Terminator profile is needed at the corporate network site. It terminates the virtual PPP link at the corporate site. The terminator profile is needed for both the voluntary and the compulsory tunnels. The peer configuration profile needs to be an L2TP Initiator profile.

# Virtual PPP Profile - Terminator



## Voluntary Tunnel Example

**New Point-to-Point Profile Properties - As20**

General | Connection | TCP/IP Settings | Authentication

Name:

Description:

The settings on this page affect the settings on the re:

Type:

- ☒ PPP
- ☐ SLIP

Mode

Line connection type:

- ☐ Switched line
- ☐ Leased line
- ☒ Virtual line (L2TP)

Mode type: **Terminator (network server)**

OK

**New Point-to-Point Profile Properties - As20**

General | Connection | TCP/IP Settings | Authentication | Subsystem

Local tunnel endpoint IP address:

Link configuration

Type of line service: Virtual line (L2TP) - terminator (network server)

Virtual line name:

Open

General | Connection | TCP/IP Settings | Authentication | Subsystem

Local IP address

- ☒ IP address:
- ☐ Dynamically assign

Remote IP address

- ☐ Dynamically assign
- ☐ IP address:
- ☐ Route specified
- ☒ Define address pool:

Starting IP address:

Number of addresses:

Routing

- ☒ Allow IP forwarding

Defines the IP address of the local L2TP tunnel endpoint (global address)

Virtual line name

Local virtual PPP connection endpoint IP address (company's address)

Remote virtual PPP connection endpoint IP address

Allows the remote L2TP client to access corporate network

# Notes: Virtual PPP Profile - Terminator



To configure a PPP profile as a L2TP Terminator, the Line Connection Type has to be Virtual line (L2TP) and the mode type Terminator (network server). Based on this selection, the following property pages contain only the parameters required for the L2TP Terminator.

The Connections page defines the characteristics of the virtual line itself. The information is specified here:

- Local tunnel endpoint IP address
  - Defines the IP address of the local end of the L2TP tunnel. It is a fixed, global routable IP address. This address must be defined as a TCP/IP interface prior to configuring the PPP profile. This address is not used for establishing user sessions.
- Virtual line name
  - The virtual line defines characteristics, such as maximum frame size, line authentication values, and so on.

The TCP/IP Settings page defines the virtual PPP link. The following parameters have to be defined:

- Local IP address
  - The local IP address defines the end of the virtual PPP link. This is the actual address used for user sessions, for example, TELNET, FTP, and so on. This address must be defined as a TCP/IP interface prior to configuring the PPP profile.
- Remote IP address
  - The remote IP address defines a single IP address, which is dynamically assigned to the remote end of the virtual PPP link. A single address is specified if the remote client is a single host. When connecting a remote branch office network, the remote IP address defines a range of IP addresses.
- Allow IP forwarding
  - IP forwarding must be enabled when the remote L2TP client wants to have full access to all hosts in the corporate network.



# **Remote VPN Clients**



## VPN Clients on the Market



- ✓ **Number of VPN clients is constantly increasing**
- ✓ **Many products include proprietary functions**
  - ▶ Vendors offer a complete solution (including clients and gateways)
  - ▶ Endangers interoperability
- ✓ **Ensure that vendor products comply with the standards**
- ✓ **Before selecting a product, try to use the vendor's customer support**
  - ▶ Gives you information about the support and response time

# Notes: VPN Clients on the Market



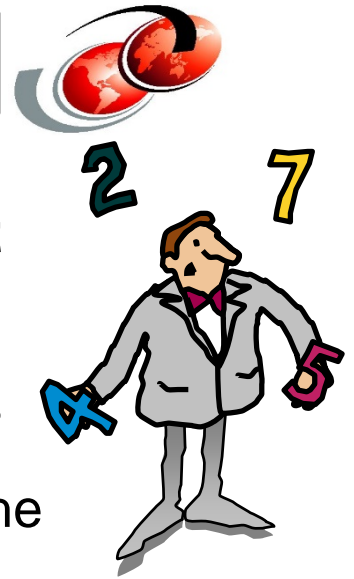
Nowadays, you find an increasing number of vendors offering VPN solutions. Many of these vendors try to offer a total VPN solution to the customer. They offer VPN clients, VPN gateways, and other security appliances that make up an entire VPN solution. To ensure that their customers buy all the components from their product suite, vendors tend to implement proprietary functions into their products. Sometimes, these functions provide some useful features that are currently not covered in any IETF standard. On the other hand, it ties the customer to one vendor.

Always try to deploy products that are RFC compliant.

Experience has shown that it is a good practice to consult, for example, the customer help desk or customer support of a vendor prior to buying a vendor's product. This gives you an impression of what to expect in case you experience problems during implementation or operation of the client software.



## Selecting a VPN client



- ✓ **Before selecting a VPN product, analyze the current customer environment and the requirements**
  - ▶ Does the remote client need an internal or private IP address?
  - ▶ Should the remote client be protected against intruders from the Internet?
  - ▶ Does the remote client have to enter the Internet through the corporate network?
  - ▶ Does the VPN client product support, at least, the IETF standards?
  - ▶ What authentication method is required?
- ✓ **The answers to these questions provide good input for the requirement profile to select a VPN client product**
- ✓ **Try to find a client product that supports IPSec and optionally L2TP**

# Notes: Selecting a VPN Client



Before you select a VPN client product, collect all the information that is needed to create a requirement profile for a VPN client product. The best starting point is the current network environment. If access to systems in the corporate network is controlled by whether the client has a certain internal network IP address, your VPN client has to support internal or private IP addresses. L2TP could be used to achieve this requirement. If you can't find a client that supports L2TP, you may want to choose a client that supports internal IP addresses, such as IRE's SafeNet Soft/PK client. Ensure that your VPN gateway supports these functions as well.

Once you know all the requirements, compare the supported functions of each VPN client product on the market. This is sometimes a painful and time-consuming process.

Ideally, you have a VPN client that supports both IPSec and L2TP.

# Remote VPN Client Products



Client	IPSec	L2TP	Dial	Eth.	TR
IRE SafeNet/Soft-PK Client <a href="http://www.ire.com">www.ire.com</a>					
Wind River Systems WinVPN Client <a href="http://www.wrs.com">www.wrs.com</a>					
Ashley Laurent VPCOM Client <a href="http://www.ashleylaurent.com">www.ashleylaurent.com</a>					
TimeStep / Newbridge Newbridge 130 Secure VPN Cl. <a href="http://www.newbridge.com">www.newbridge.com</a>					
RADGUARD clPro Client <a href="http://www.radguard.com">www.radguard.com</a>					
Microsoft Windows 2000 <a href="http://www.microsoft.com">www.microsoft.com</a>					

# Notes: Remote VPN Client Products



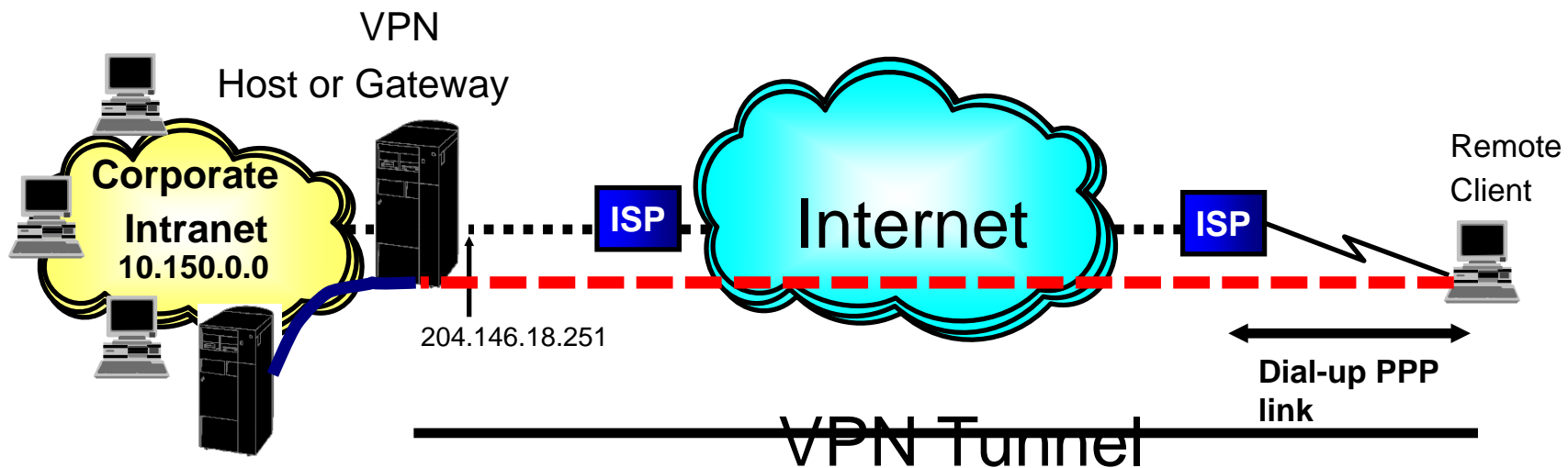
The chart shows some of the available VPN clients on the market and is meant to provide an overview of the clients with their major supported functions. The order of the clients in the table are not related to a priority or preference. Before you decide to buy one of the clients, we recommend that you always get an evaluation version prior to purchasing one.

All vendors change their products frequently. Check their Web pages for information about their current supported functions.

# VPN Remote Client Configuration



- ✓ Typically the remote client uses dynamically assigned addresses
- ✓ Transparent to ISP



- Traffic protected by VPN
- Traffic flows in the clear (unless it is a VPN Host to Host connection)

- ✓ IP address assigned from ISP
- ✓ PC uses an identifier other than an IP address
  - e-mail address
  - Fully qualified domain name
  - other identifiers

# Notes: Remote VPN Client Configuration



In a typical remote client environment, the remote PC dials into an ISP's Point of Presence (PoP). The ISP dynamically assigns an IP address to the client. The link between the PoP and the client is a PPP link. Even if the remote PC uses the same ISP PoP, it is likely that the PC is assigned a different IP address every time. This makes it impossible to identify a remote client on the VPN gateway site by its IP address. Therefore, other identifier types are required to uniquely identify the remote client to the VPN gateway. The AS/400 system supports the following identifier types for a dynamic IP user environment:

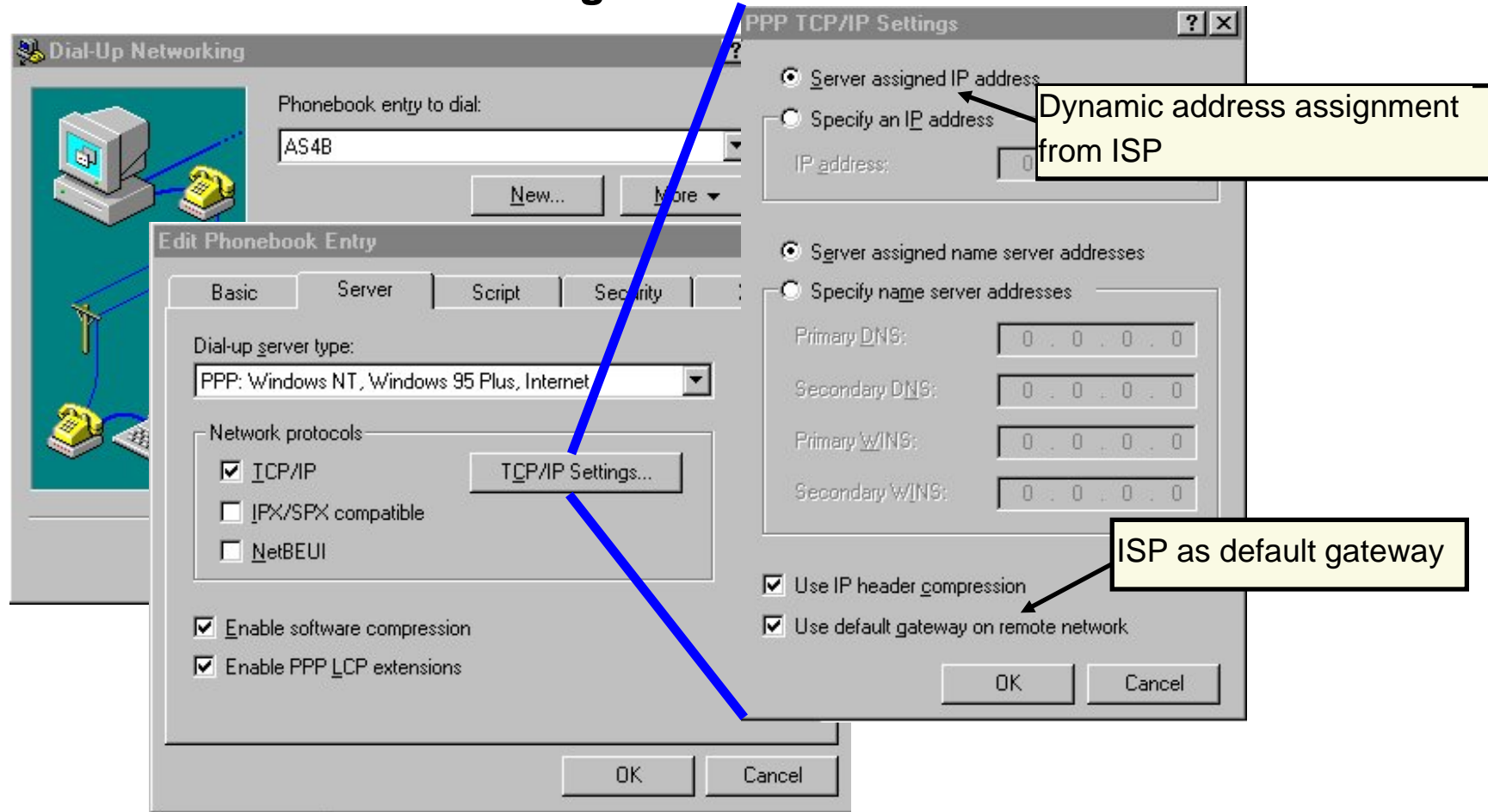
- e-mail address (User@FullyQualifiedDomainName - User@FQDN - Identifier type 3)
- key identifier (Key ID - Identifier type 11)

✓**Note:** Not all VPN clients support these identifier types. Most of them received the e-mail address identifier added in newer releases. When selecting a remote VPN client, make sure that it supports the necessary identifier types.

# Remote Client PPP Configuration



- ✓ Asynchronous connections
- ✓ PPP Authentication through ISP







# AS/400 VPN Configuration



✓ Use the configuration wizard Gateway to Dynamic IP Users

The screenshot shows the 'Virtual Private Networking - As4b' window. The 'New Connection...' menu is open, and 'Gateway To Dynamic IP Users' is selected. A summary window is displayed on the right, showing the configuration details for a dynamic IP user connection group named 'TechnicalSupportGroup1'. The summary includes the following information:

- Dynamic IP user connection group name: TechnicalSupportGroup1
- Users: Authentication: Pre-shared key; Identifier type for users: User @ fully qualified domain name; barlen@us.ibm.com marion@company.com
- Data Policy: Highest security
- Key Policy: Highest security
- Local key server: Identifier type: Version 4 IP address; IP Address: 204.146.18.251

The summary window also lists the objects that will be created:

- Dynamic IP Connection Group: TechnicalSupportGroup1
- Key Connection Group: TechnicalSupportGroup1
- Data Policy: TechnicalSupportGroup1HS
- Key Policy: TechnicalSupportGroup1HS

Annotations on the image include:

- A yellow box with the text 'Identifier type: e-mail address' pointing to the 'Identifier type for users' field in the summary window.
- A yellow box with the text 'Created objects for remote clients' pointing to the list of objects that will be created.
- A red box labeled 'B' highlighting the user list in the summary window.
- A red box labeled 'A' highlighting the list of objects that will be created.

# AS/400 VPN Configuration (cont'd)



## ✓ Verify key and data policies

**Key Protection Transform** D

Authentication method: Pre-shared key

Hash algorithm: SHA

Encryption algorithm: 3DES-CBC

Diffie-Hellman group: Default 768-bit MODP

Key management

Maximum key lifetime: 60 minutes

Maximum size limit: No size limit kilobytes

Configuration values of key and data policy are needed for VPN client configuration

**Data Protection Proposal** E

General | Key Expiration

Transforms

Protocol	Authentication Algorithm	Encryption Algorithm
ESP	HMAC-SHA	3DES-CBC

Encapsulation mode

☒ Tunnel

☐ Transport

**Data Protection Proposal**

General | Key Expiration

Key expiration

Expire after: 30 minutes

Expire at size limit: No size limit kilobytes

# AS/400 VPN Configuration (cont'd)



## ✓ Change the Dynamic IP Group - Policy settings

Properties - TechnicalSupportGroup1

General | Users | Associations | Policy | Address Translation

Data management security policy:

TechnicalSupportGroup1HS [New] [Properties]

These values that define the traffic for active connections come from:

Local addresses: Filter rule

Local ports: Connection

Remote addresses: Connection

Remote ports: Connection

Protocol: Connection

Connection lifetime: Never expires minutes

Restrict access to subnets

Restrict access to applications

# Notes: AS/400 VPN Configuration



The easiest way to configure the AS/400 system as a VPN gateway for remote VPN clients is by using the New Connection Wizard. The wizard creates all the required configuration objects.

When running the New Connection Wizard, you have to select the security level you want to use for the key and data policy. After the wizard completes the creation of the required objects, make sure to edit the key and data policy and write down all the configuration values. The values will be needed when configuring the VPN client.

One of the most important changes is made in the Dynamic IP Group. On the Policy page of this group, you define the access restrictions that apply to the remote client to the corporate network. For example, if you want to restrict remote clients to access the corporate subnet 10.150.10.0 only, you have to define the appropriate filter rule and select the value Filter Rule on the Local Addresses parameter. The same applies for ports or protocols. The only value that usually needs to be set to Connection is the value for the Remote Addresses parameter, because in a dynamic IP environment you cannot predict the remote IP address.

# AS/400 IP Packet Security



AS/400 Operations Navigator

File Edit View Options Help

Environment: My AS/400 Connection

My AS/400 Connection

- As01
- As25
- As4a
- As4b
  - Basic Operations
  - Job Management
  - Configuration and S
  - Network
    - IP Security
      - Point-to-Point
      - Modems
      - Connection
      - Protocols
      - Servers
      - IBM Network S
      - Internet
    - Security
    - Users and Groups
    - Database
    - File Systems
    - Multimedia
    - Backup
    - Application Develop
  - As4c
  - Asa

Server Name	Status	Description
IP Packet Security	Inactive	IP packet security filter rules
Virtual Private Networking	Started	Secure connections and policies

IP Packet Security - As4b

File Edit View Help

New Rules File

- IP Packet Security
  - All Security Rules
  - Defined Addresses
  - Filter Interfaces
  - Filters
  - Services
  - Address Translation
  - Includes
  - Comments

IP Packet Security: All Security Rules

Statement
-----------

Be very **careful** when activating IP Filters...you can stop some or all IP traffic if you make a mistake.

1 - 2 of 2 object(s)

# AS/400 IP Packet Security (cont'd)



New Defined Address - As4b

General

Address name: Subnet10150

Interface specification

☐ Interface names:

☒ IP specification:

Subnet mask: 255.255.0.0

☒ IP addresses: 10.150.0.0

☐ Start address:

☐ Local

Type: TRUSTED

Description: Internal subnet

OK Cancel Help

C

Create a defined address for the corporate intranet subnet

# AS/400 IP Packet Security (cont'd)



Create an inbound and outbound filter rule for IKE

The image displays three screenshots of the 'New Filter - As4b' dialog box, illustrating the configuration of filter rules for IKE traffic.

**Top Left Screenshot (Inbound Filter):**

- General Tab:**
  - Set name: VPNClients
  - Action: PERMIT
  - Direction: INBOUND
  - Source address name: = \*
  - Destination address name: = 204.146.18.251
- Services Tab:**
  - Service: ☒ Service
  - Protocol: UDP
  - Source port: = 500
  - Destination port: = 500

**Top Right Screenshot (Outbound Filter):**

- General Tab:**
  - Set name: VPNClients
  - Action: PERMIT
  - Direction: OUTBOUND
  - Source address name: = 204.146.18.251
  - Destination address name: = \*
- Services Tab:**
  - Service: ☒ Service
  - Protocol: UDP
  - Source port: = 500
  - Destination port: = 500

**Bottom Screenshot (Filter Rule Summary):**

- General Tab:**
  - Set name: VPNClients
  - Action: PERMIT
  - Direction: INBOUND
  - Source address name: = \*
  - Destination address name: = 204.146.18.251
- Services Tab:**
  - Service: ☒ Service
  - Protocol: UDP
  - Source port: = 500
  - Destination port: = 500



# AS/400 IP Packet Security (cont'd)



Create the IPsec filter rule

**New Filter - As4b**

General Services

Set name: VPNClient

Action: IPSEC

Direction: OUTBOUND

Source address name: = Subnet10150

Destination address name: = \*

Fragments: NONE

Journaling: OFF

Connection name: DYNAMICIP

Filter - As4b

Services

☐ Service name:

☒ Service:

Protocol: \*

Source port: = \*

Destination port: = \*

Remote clients have access to local subnet 10.150.0.0 only

Required for all dynamic IP connections and can be specified only once

**Properties - TechnicalSupportGroup1**

General Users Associations Policy Address Translation

Data management security policy:

TechnicalSupportGroup1HS

New

Properties

Local addresses: Filter rule

Local ports: Connection

Remote addresses: Connection

Remote ports: Connection

Protocol: Connection

Configuration on the client must match

Connection = Values not taken from filter rules



# Notes: AS/400 IP Packet Security



IP Packet Security is essential to VPN on the AS/400 system. The New Connection Wizard does not configure filter rules. Filter rules have to be created manually. Note that, whenever you add any filter rules for an AS/400 line description, the system automatically adds a DENY ALL default for that line. This means any traffic not explicitly permitted will be denied. You cannot see or change this rule. As a result, you may find that connections which previously worked, mysteriously fail once filter rules have been activated. From a security viewpoint, default DENY is a sound policy, particularly if the AS/400 system is to be directly connected to the Internet. In the worst case, however, you might accidentally restrict access to the line you use for AS/400 Operations Navigator and, therefore, not be able to deactivate IP Filtering to fix the problem. In this case, the RMVTCPTBL \*ALL command can be used from a green screen to deactivate all filter rules.

The basic filter rules required are the IKE and IPSec filter rules. You can create one IKE filter rule that serves all IKE communication. In this case, you would specify the wildcard character "\*" for Direction, Source and Destination address. But we do not recommend this. Always try to limit access to your system as much as possible. The IPSec filter rule for dynamic IP users must have the DYNAMICIP value specified in the Connection Name parameter. Note that a single connection name can be specified only once in a filter rule file. Therefore, your network and security scheme must be configured to reflect this requirement. Note that you cannot define multiple non-contiguous subnets for one IPSec filter rule.

The Policy page of the Dynamic IP Group defines how the VPN connection will be established and which party takes control of the allowed configuration values. For example, you have an IPSec filter rule that allows access from remote clients to the local subnet 10.0.0.0. You have defined Connection for Local Addresses on the Policy page. The client is now able to either configure the subnet 10.0.0.0 or a subset (10.150.0.0, 10.4.0.0, etc.) and still get access. When you specify Filter Rule for Local Addresses in the Policy settings, the VPN connection will not be established. In this case, the configuration of the IPSec filter rule and the PC has to match.

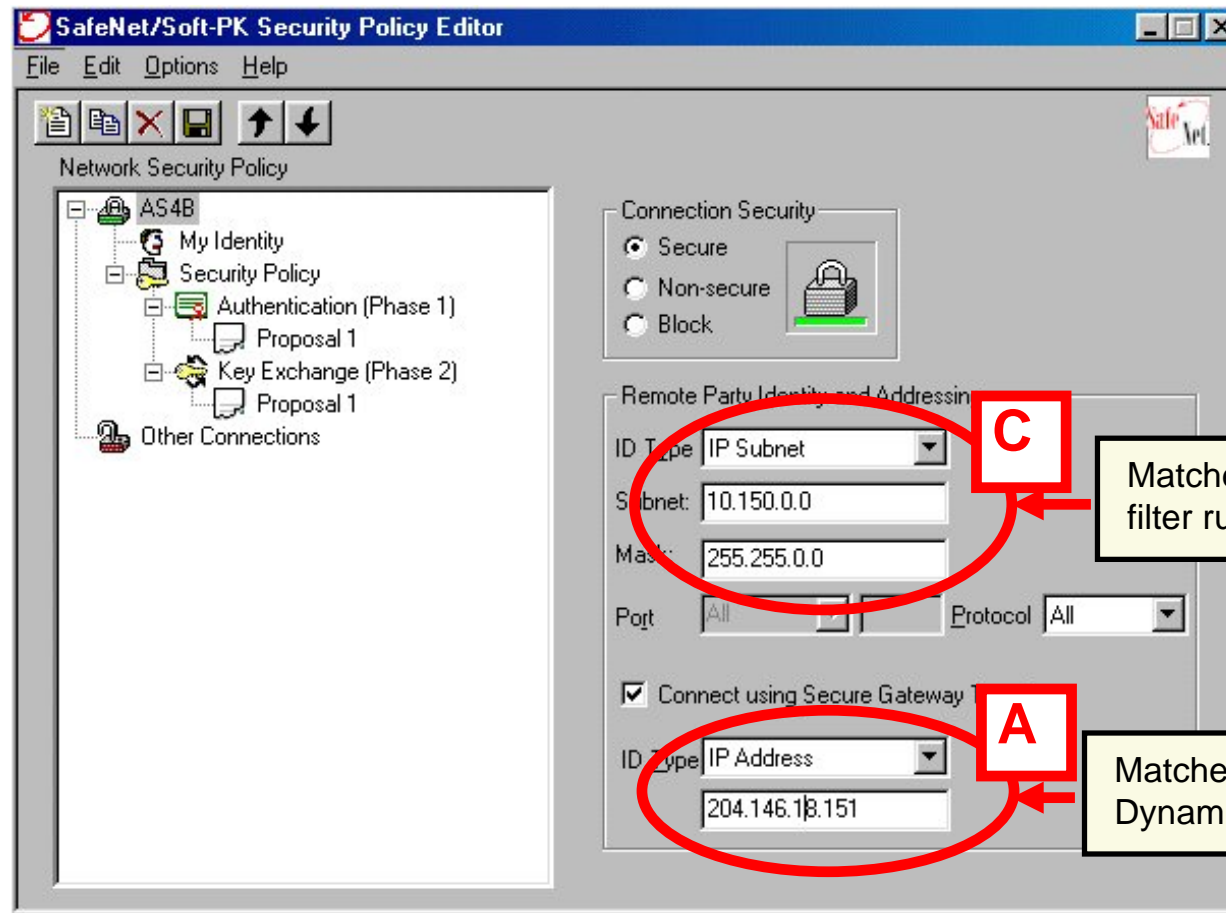
# SafeNet Soft-PK VPN Client



**The configuration in this example is based on the  
SafeNet Soft-PK client from IRE**

- Available for a "long" time in the market
- Supports main mode, aggressive mode, and manual keys
- Includes an Internal Network IP Address feature
  - Allows to use internal corporate network IP addresses for remote clients
- Does not support L2TP
- Supports only dial-up and Ethernet connections
- Intuitive configuration interface

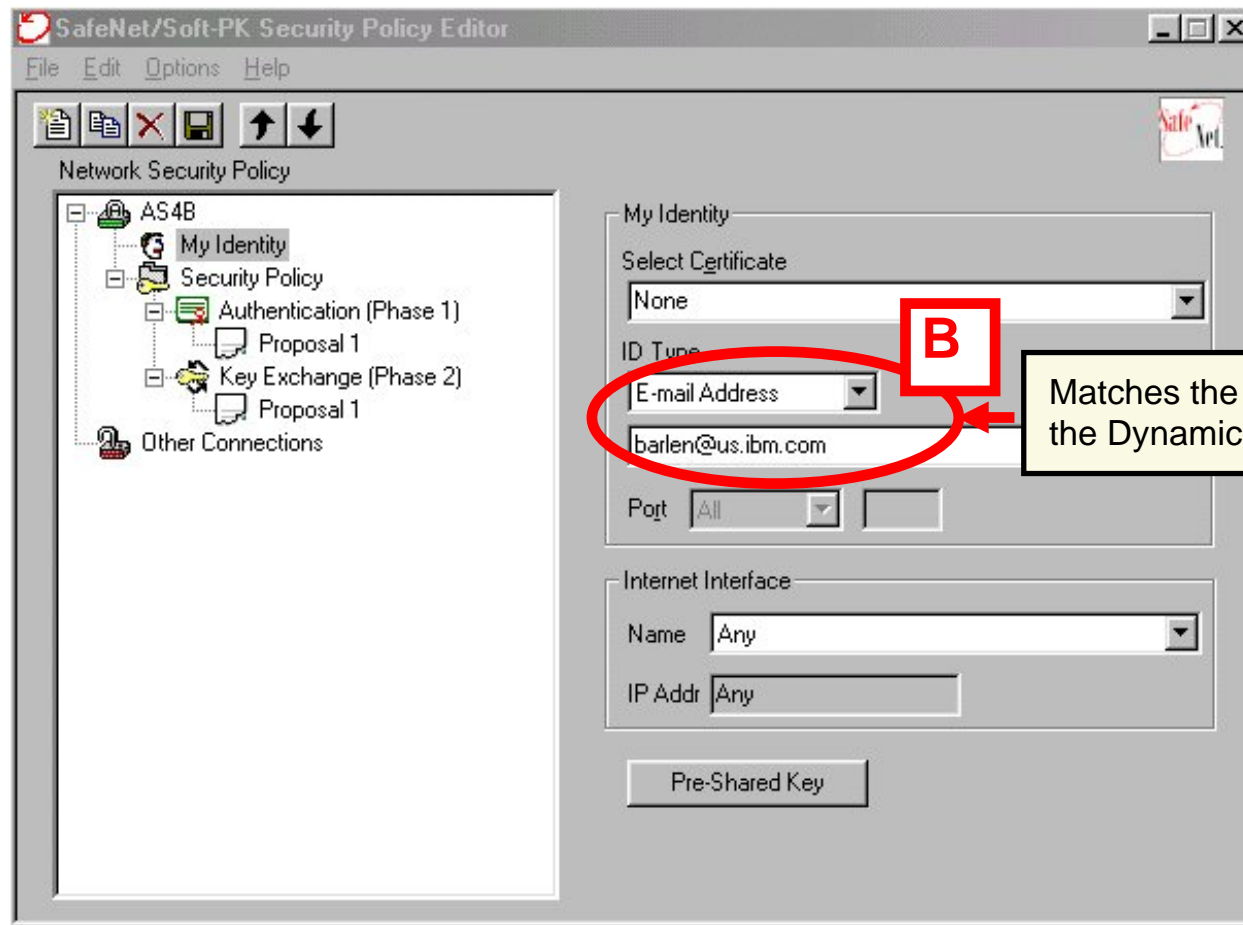
# SafeNet Soft-PK - New Connection



Matches the defined address/IPSec filter rule

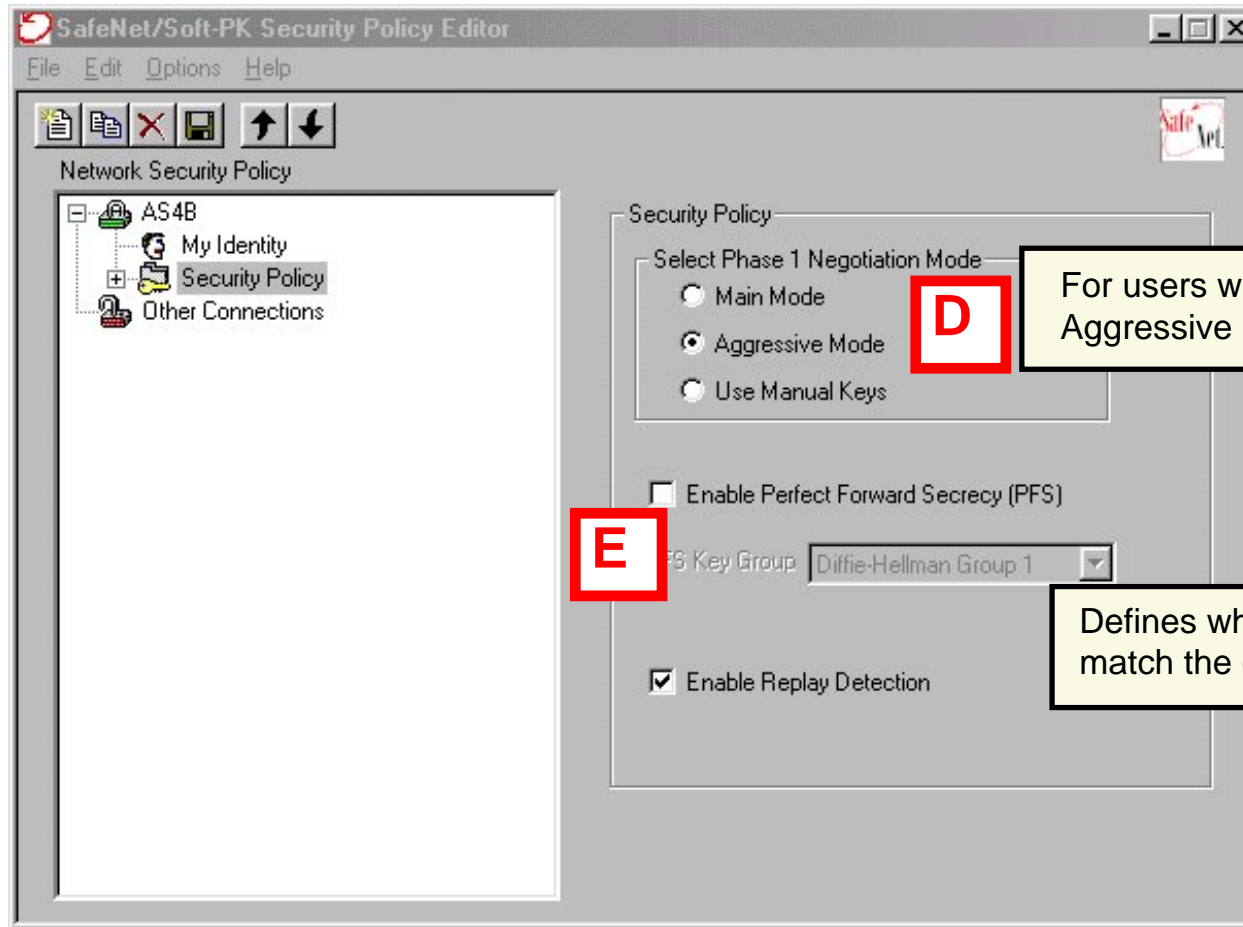
Matches the Local Identifier of the Dynamic IP Group

# SafeNet Soft-PK - My Identity



Matches the Remote User Identifier of the Dynamic IP Group

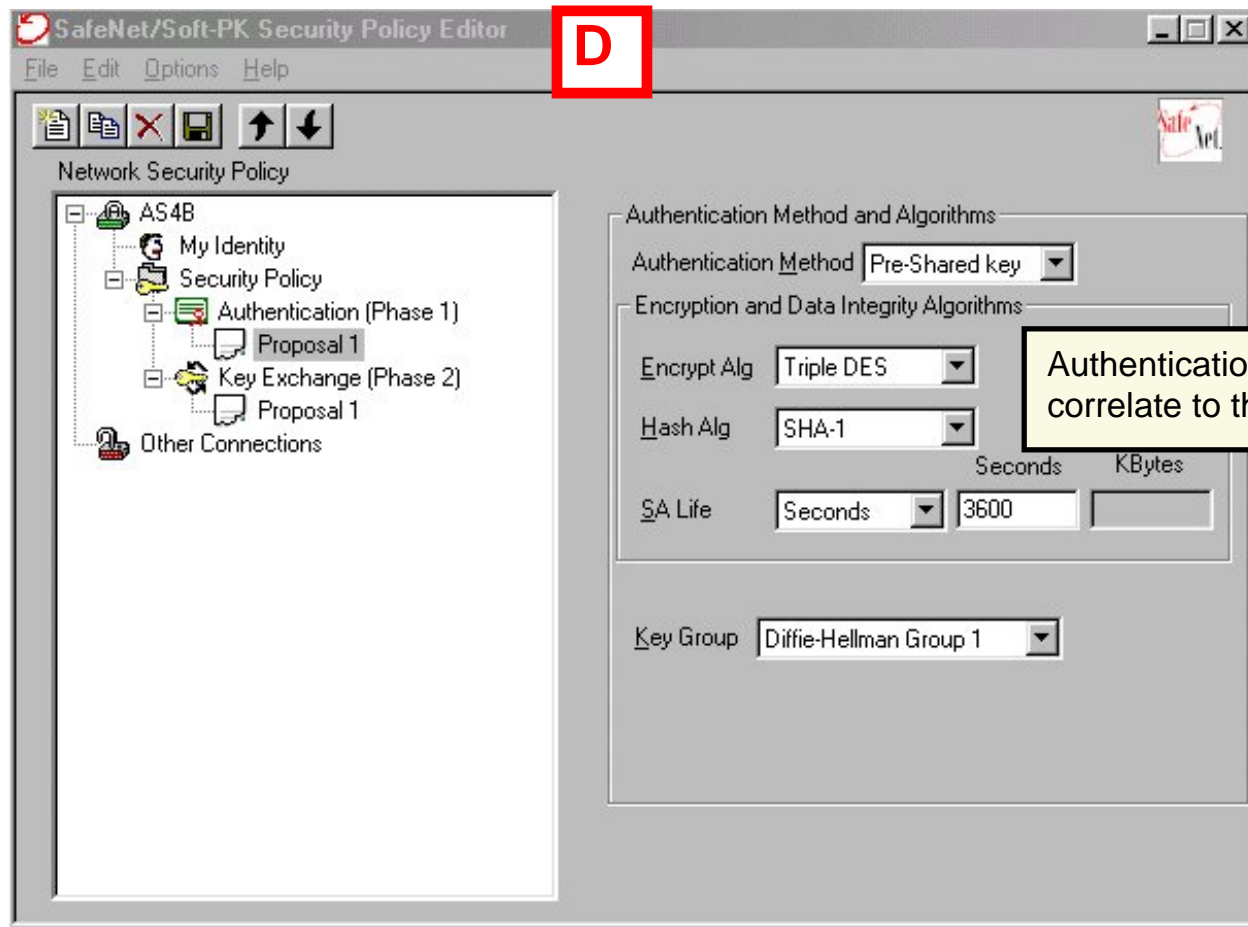
# SafeNet Soft-PK - Security Policy



For users without a fixed IP address, use the Aggressive Mode as defined in the Key Policy

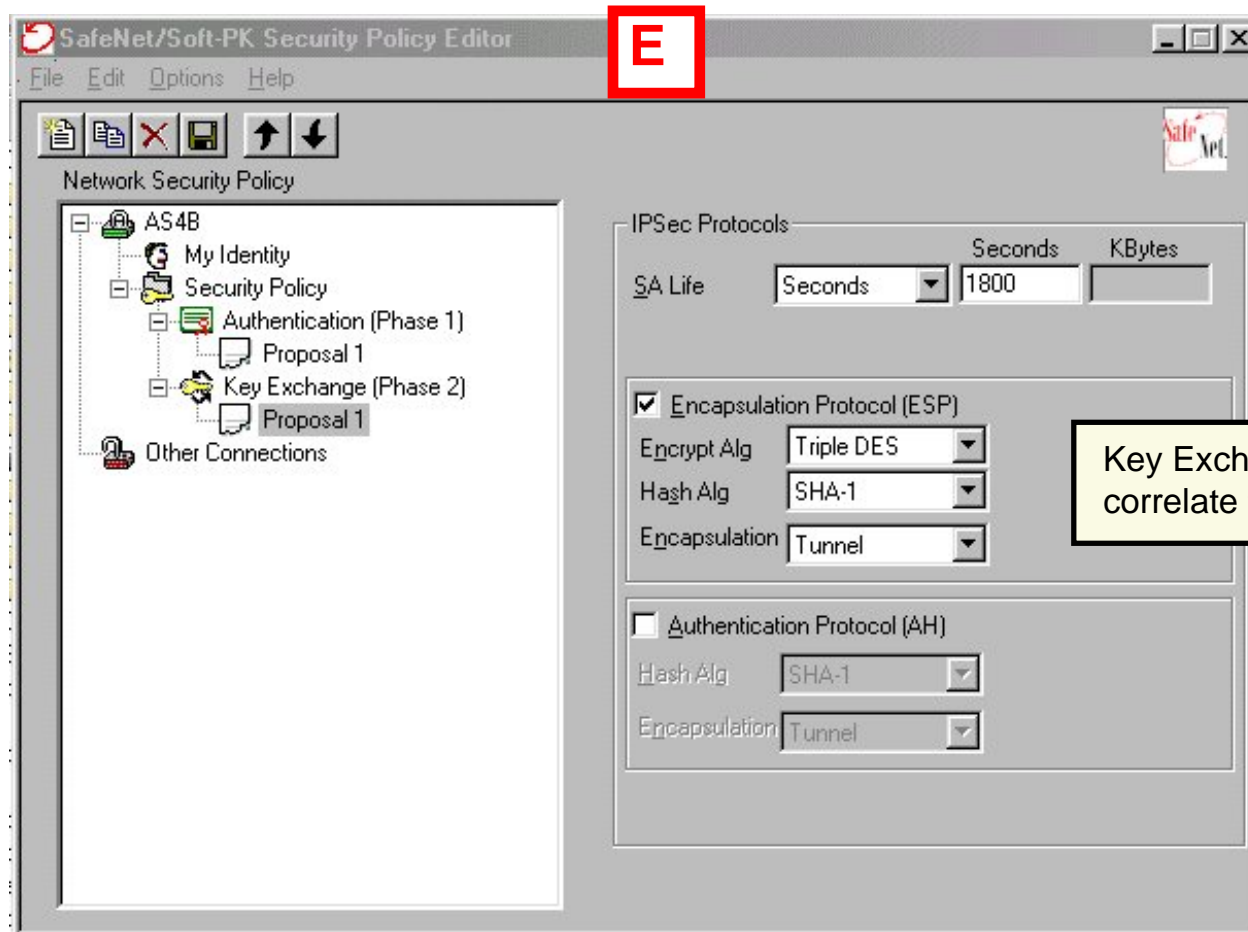
Defines whether PFS is used and must match the configuration in the Data Policy

# SafeNet Soft-PK - Security Policy - Phase 1



Authentication (Phase 1) Proposals  
correlate to the Key Policy

# SafeNet Soft-PK - Security Policy - Phase 2



Key Exchange (Phase 2) Proposals  
correlate to the Data Policy

## Notes: SafeNet Soft-PK client



The configuration windows shown for the remote client are from the SafeNet Soft-PK client from IRE. As you have seen on the previous charts, some of the terms used on the AS/400 system and on the client are different. Nevertheless, the policy configuration values for the key (phase 1) and data policy (phase 2) are quite the same. The configuration example shown in this presentation proves that somebody who plans and implements client VPN solutions must be familiar with the technology and the common terminologies used in this environment. Otherwise, they may not be able to configure such a VPN connection. Even worse, if you don't understand all the functions, you can open a security hole without knowing it.



# Windows 2000 - VPN Client



**The configuration in this example is based on the  
Windows 2000 client from Microsoft**

- VPN limitations in dial-up environments
  - Windows 2000 supports only main mode with pre-shared key
  - Dynamically assigned IP addresses require certificate-based authentication
  - With OS/400 V4R4 you can only use fixed client IP addresses
  - Enhancement in OS/400 V4R5 to allow an IP address range for remote clients
- Supports L2TP and IPsec
- VPN capabilities built in base Windows 2000 operating system...just like OS/400 always had
- Connection support for dial-up, Ethernet, and Token Ring networks
- Requires Microsoft Management Console (MMC) for configuration
  - Wizards available for L2TP and IPSec configuration

## Windows 2000 - VPN Client (cont'd)



- AS/400 Host to Hosts configuration wizard can be used to create all required VPN configuration objects
  - Changes to the objects are required
- V4R5 IP address range enhancement requires all remote clients to share the same pre-shared key
  - Use CHAP for L2TP user authentication

# Notes:



## AS/400 and Windows 2000 VPN compatibility

- AS/400 V4R4 IPSec can only establish a VPN connection with Windows 2000 if the client is assigned a fixed IP address. The reason for this limitation is that Windows 2000 does not support IKE aggressive mode (only main mode is supported). For a dynamically assigned IP address, Windows 2000 requires certificate-based authentication.
- The AS/400 system only supports pre-shared key authentication in V4. To solve this problem and be able to establish IPSec tunnels between the AS/400 system and Windows 2000 clients, AS/400 VPN support has been enhanced in V4R5 to allow a range of IP address as remote identifier. This allows you to configure the range of possible IP address that the ISP may assign to the client and continue using pre-shared key as the authentication method. The disadvantage of using an IP address range is that all clients share the same pre-shared key during Internet Key Exchange (IKE) authentication. To bring back individual user authentication, you have to configure CHAP (Challenge Handshake Authentication Protocol) for the L2TP tunnel connection.

With Windows 2000 you can secure an L2TP tunnel using the IPSec protocol suite, which means that you extend the corporate network to the remote client site while securing (for example, using IPSec encryption) the L2TP tunnel traffic.

You can use the VPN Host to Hosts configuration wizard to create all required configuration objects on the AS/400 system. Some modifications need to be done in the Key Policy, Key Connection Group, and Dynamic Key Group to connect Windows 2000 to the AS/400.

# OS/400 VPN Enhancement



**New IP Address Range support required on AS/400 for Windows 2000**

Properties - Windows2000

General Associations Address Translation

Name: Windows2000

Description: Allow remote L2TP client connections

Remote server identifiers:

Type	Identifier
IP version 4 address range	0.0.0.0-255.255.255.255

Add

Edit

Remove

Set Pre-shared Key

Pre-shared Keys...

OK Cancel Help

# Windows 2000 - VPN Management



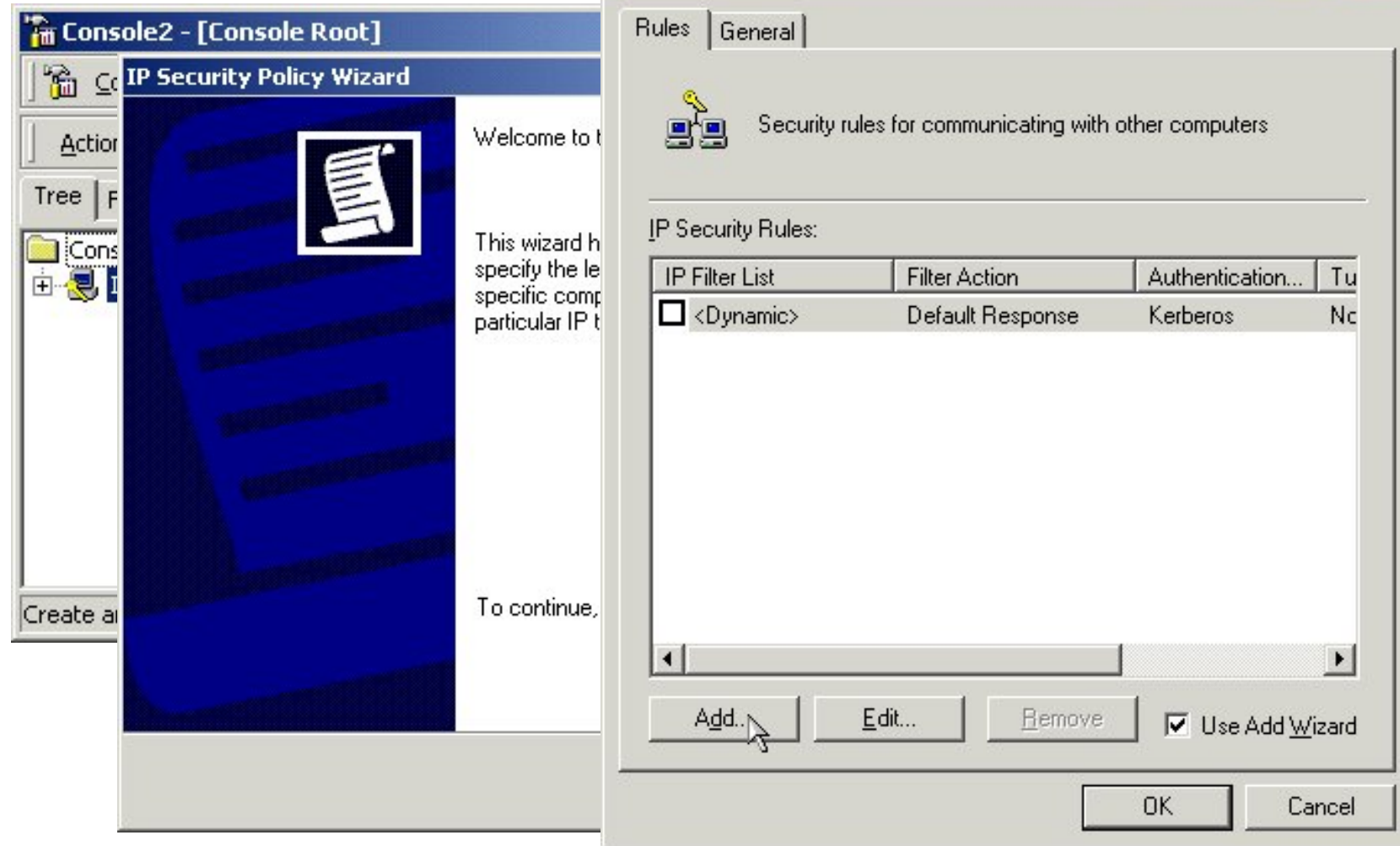
**MMC snap-in IP Security Policy Management is required to configure L2TP and IPSec on Windows 2000**



# Windows 2000 - Configuration wizards



**Single MMC option starts a series of configuration wizards to configure a VPN under Windows 2000**



# Windows 2000 - IP Filter wizard



**IP Filter wizard defines which traffic will be protected by the VPN connection**

**Filter Wizard** [?] [X]

**IP Filter List** [?] [X]

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: AS25b\_Filter List

Description:

Filters: ☒ Use Add Wizard

Mirrored	Protocol	Source Port	Destination Port	Source Address	Source Mask	Destination Address	Destination Mask
Yes	UDP	1701	ANY	<My IP Address>	255.255.255.255	204.146.16.71	255.255.255.255

Close Cancel

## Notes:



The IP Filter wizard creates filter rules that specify how data traffic is treated on Windows 2000 VPN. You have to specify which traffic should be protected. Incoming and outgoing filter rules must be defined. The Mirrored option of the IP Filter wizard creates automatically the corresponding filter rule. For example, if you create a filter rule where the source address is the PC and the destination address is the AS/400 system, the wizard creates implicitly the corresponding inbound rule.

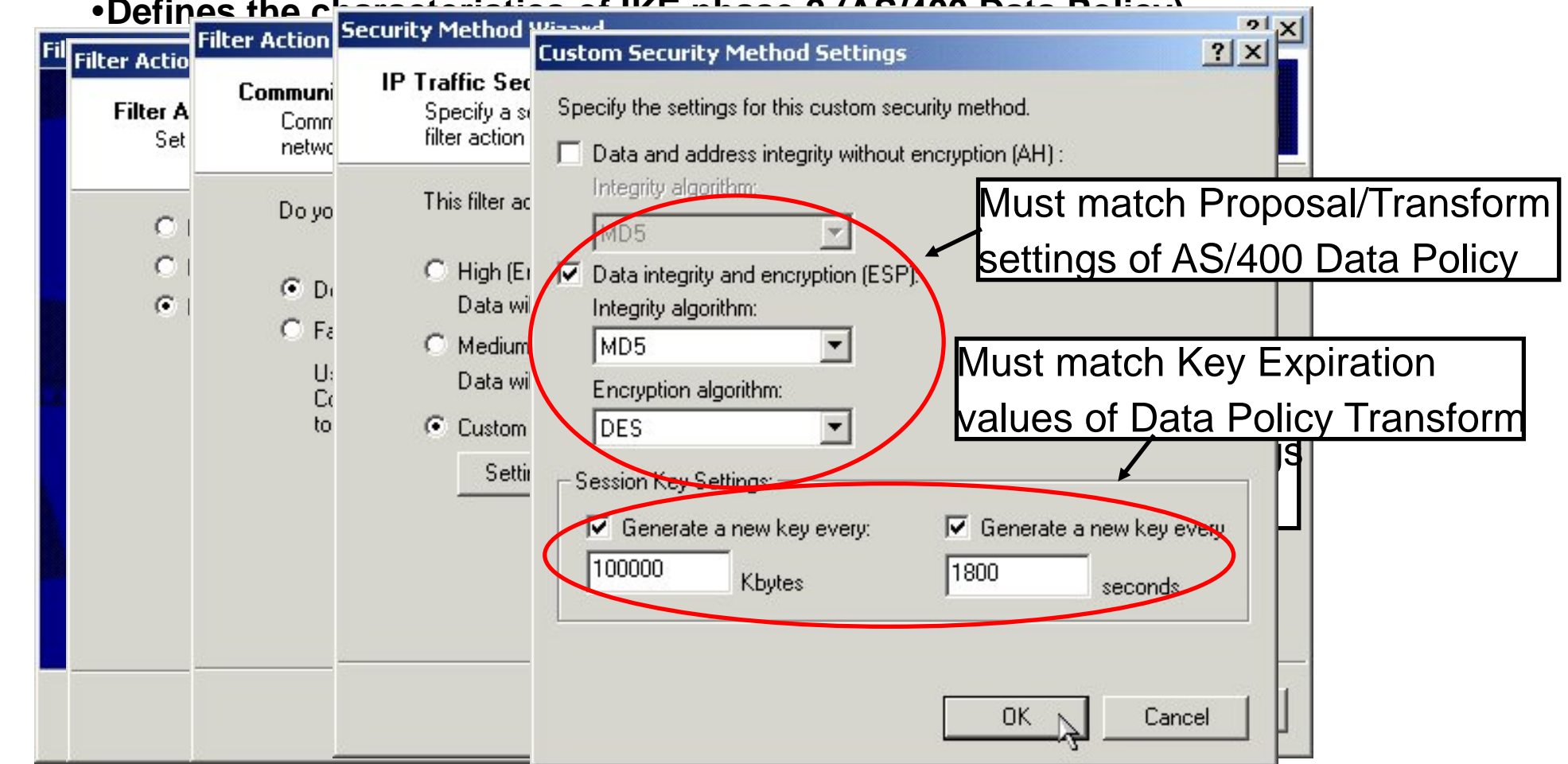


# Windows 2000 - IP Filter action



## Configuring the IP Filter action

- Defines if data traffic will be denied, permitted, or secured
- Defines the characteristics of IKE phase 2 (AS/400 Data Policy)



Filter Action Wizard

Filter Action: Filter A Set

Community: Comm network

Do you want to:

- ☐ Deny
- ☐ Permit
- ☒ Filter

IP Traffic Security

Specify a security filter action

This filter action:

- ☐ High (Encryption)
- ☐ Medium (Encryption)
- ☒ Custom

Settings

Custom Security Method Settings

Specify the settings for this custom security method.

☐ Data and address integrity without encryption (AH):

Integrity algorithm: MD5

☒ Data integrity and encryption (ESP):

Integrity algorithm: MD5

Encryption algorithm: DES

Session Key Settings:

☒ Generate a new key every: 100000 Kbytes

☒ Generate a new key every: 1800 seconds

OK Cancel

Must match Proposal/Transform settings of AS/400 Data Policy

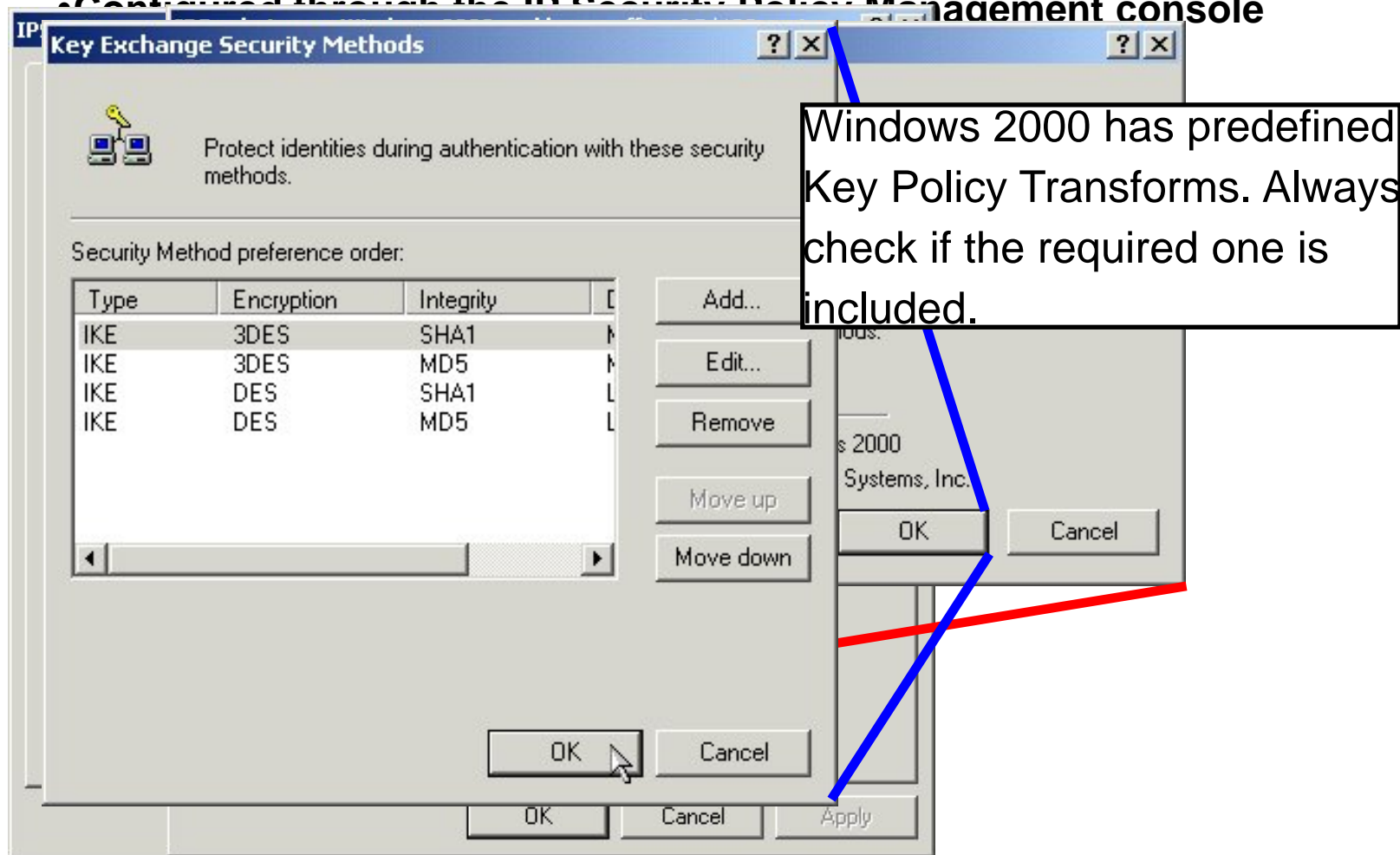
Must match Key Expiration values of Data Policy Transform

# Windows 2000 - Key Exchange



## Configuring the key exchange settings

- Defines the characteristics of IKE phase 1 (AS/400 Key Policy)
- Configured through the IP Security Policy Management console

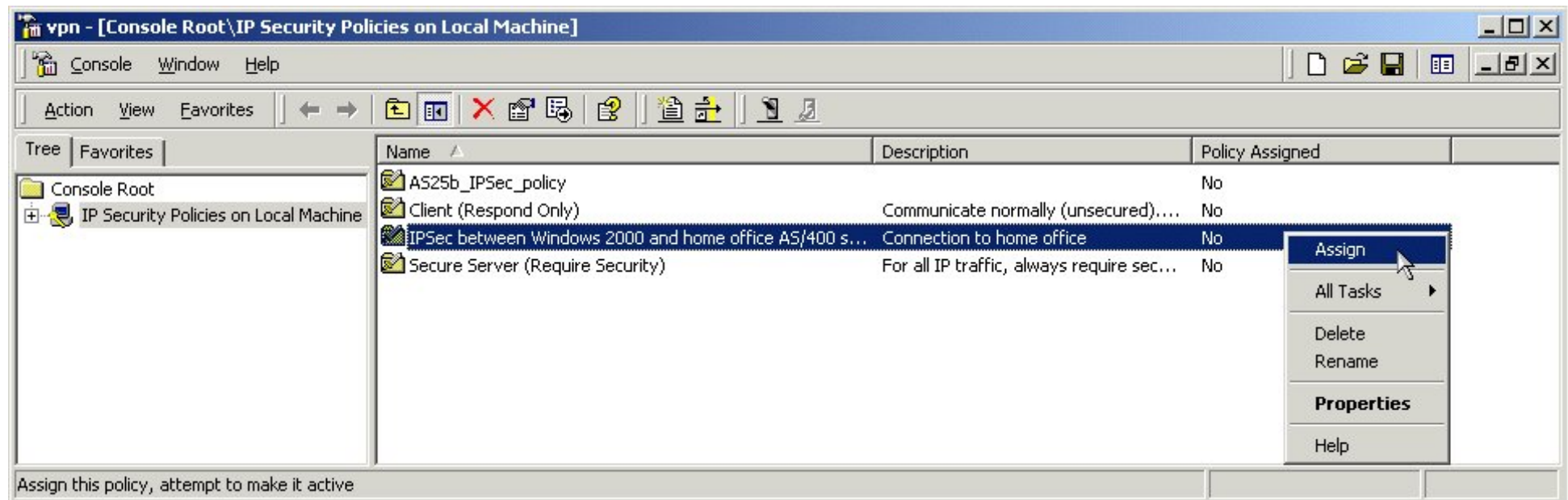


# Windows 2000 - Assigning the policy



## Activating the desired policy

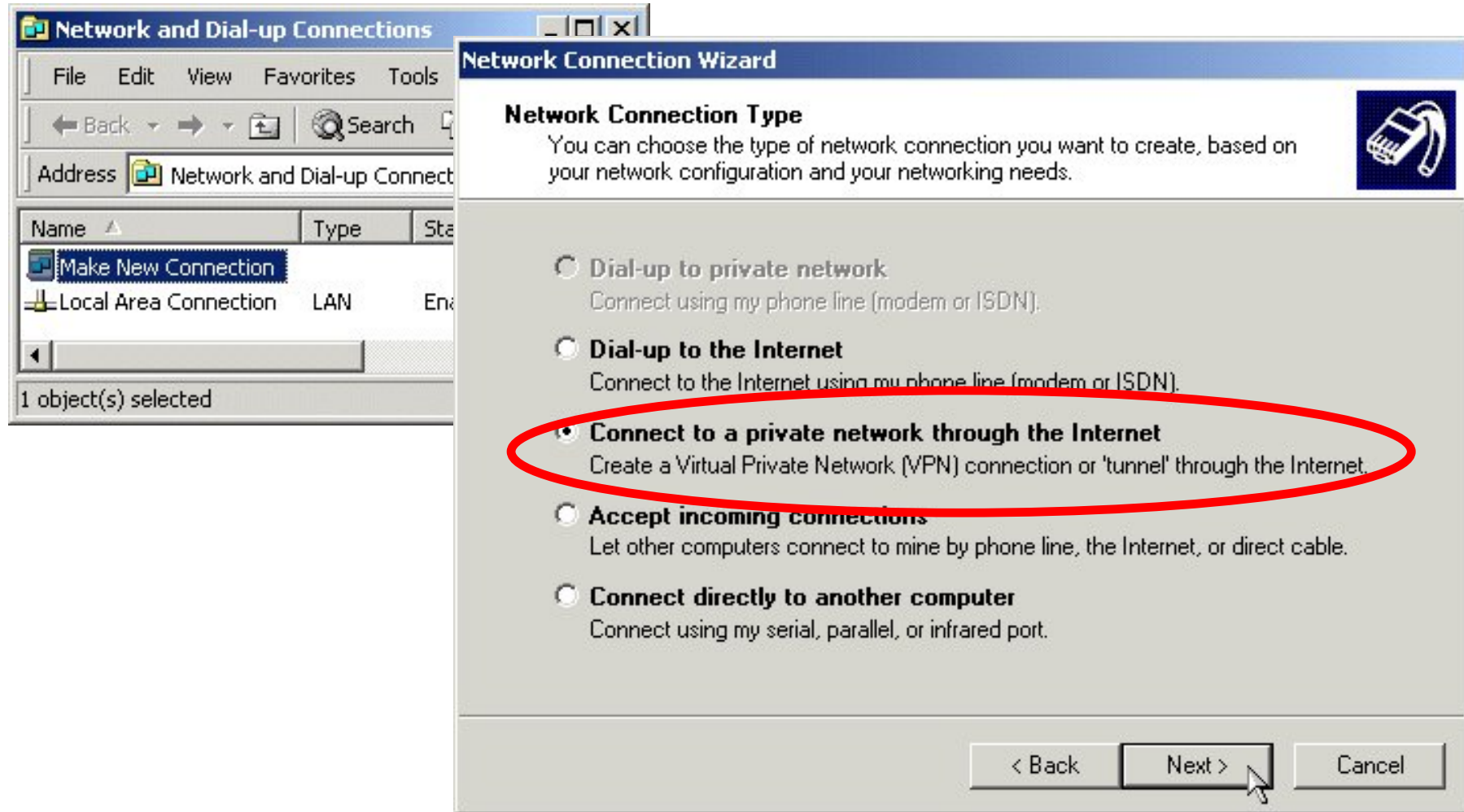
- The created policy must be assigned within the IP Security Policy Management console



# Windows 2000 - L2TP Configuration



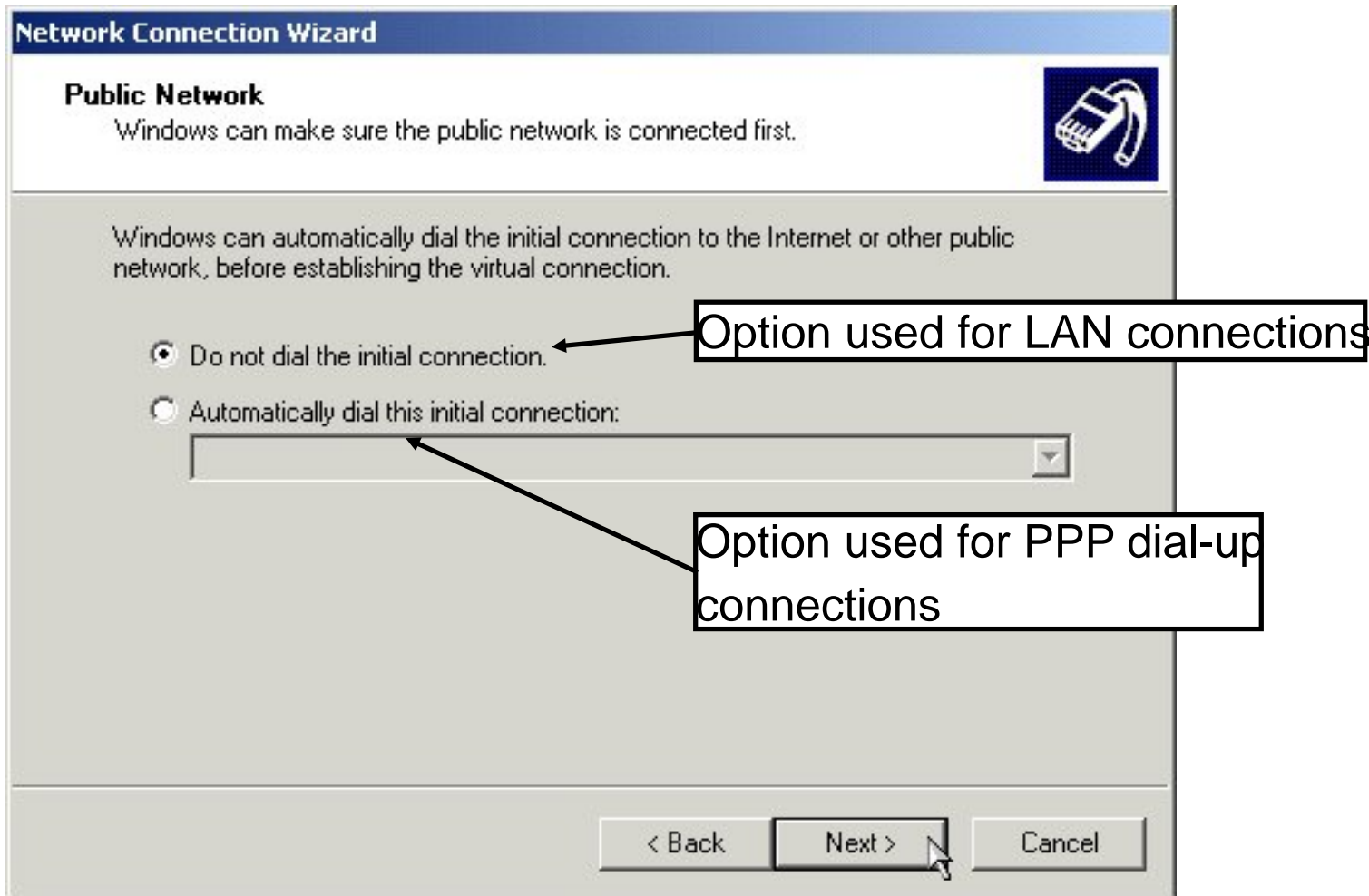
**Network Connection Wizard is used to configure L2TP on Windows 2000**



# Windows 2000 - L2TP Configuration



Wizard creates an L2TP configuration for LAN or dial-up connections



**Network Connection Wizard**

**Public Network**  
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

☒ Do not dial the initial connection. ← Option used for LAN connections

☐ Automatically dial this initial connection:  
↓ Option used for PPP dial-up connections

< Back   Next >   Cancel

# Windows 2000 - L2TP Tunnel endpoint



**Network Connection Wizard**

**Destination Address**  
What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):

204.146.16.71

< Back   Next >   Cancel

Defines the tunnel endpoint. In this case the tunnel terminates at the AS/400 system



# Windows 2000 - L2TP Availability



**Network Connection Wizard**

**Connection Availability**  
You may make the new connection available to all users, or just yourself.

You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

☒ For all users

☐ Only for myself

< Back   Next >   Cancel

Defines by whom this L2TP connection can be used

# VPN Client configuration examples



**You want to know more about how to configure a Windows 2000 or a SafeNet Soft-PK client?**

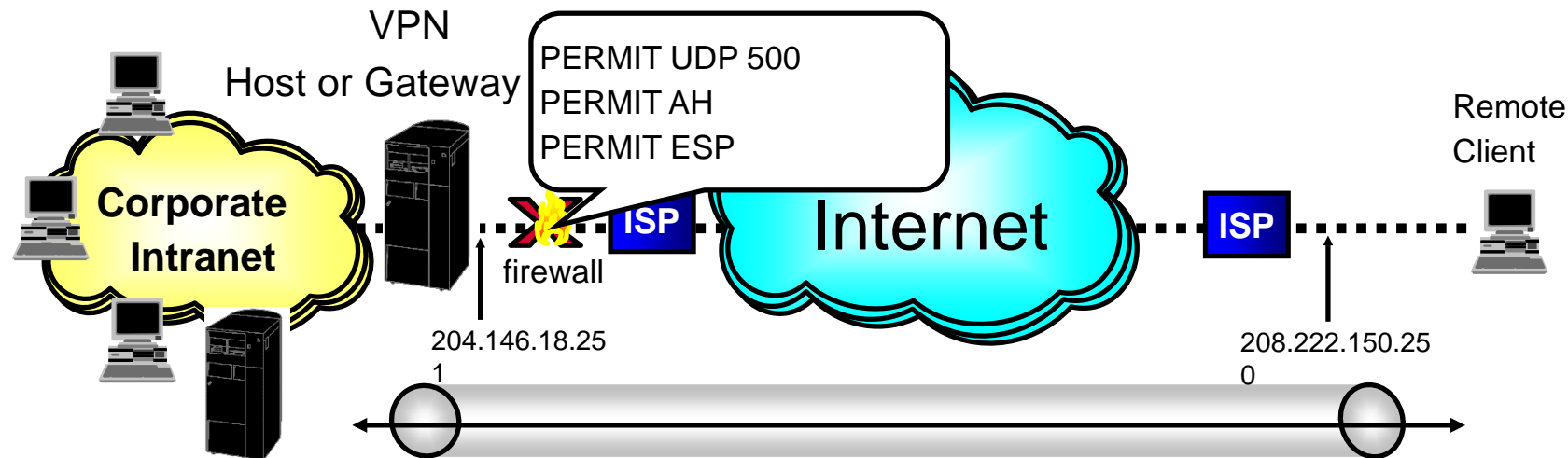
- **You can find configuration examples in the following redbooks:**
  - **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404**
  - **AS/400 Internet Security: Network Security Scenarios - A Practical Guide, SG24-5954 (to be published later in 2000)**
- **Join the Forum 2000 lab session "L41- Configuring a Remote VPN Client" to see how a SafeNet Soft-PK client is configured for a connection to an AS/400 VPN gateway.**



**Notes:**



# VPN through a Firewall



- ✓ Firewall required at one or both remote locations for connection to Internet
- ✓ Use IPsec on firewall(s), but...
- ✓ ...if the firewall doesn't support (a compatible implementation of) IPsec, you need to define IP filters to permit IPsec traffic through to an AS/400 VPN server
- ✓ Firewall filters need to recognize AH and ESP protocols

# Notes: VPN through a Firewall



In a scenario where the firewall is not the VPN endpoint, or doesn't support VPN, you have to open the firewall for the IPSec protocols AH (protocol number 51), ESP (protocol number 50), or both. In addition, you have to allow UDP traffic on port 500 for IKE negotiations.



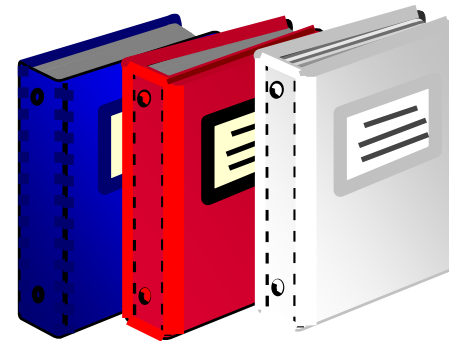
# **Publications**

# ITSO Web Page



**[HTTP://WWW.REDBOOKS.IBM.COM](http://www.redbooks.ibm.com)**

- Redpieces
- Redbooks
- Residencies



# Related Publications



- *The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this workshop.*

## International Technical Support Organization Publications

- For information on ordering ITSO publications, visit us at <http://www.redbooks.ibm.com> (Internet Web site)  
or
- <http://w3.itso.ibm.com> (intranet Web site)

For Technical Support see <http://www.ibm.com/support> and <http://w3.ibm.com/support>

## Redbooks on CD-ROMs

- Redbooks are available on CD-ROMs.

### CD-ROM Title

### Collection Kit Number

System/390 Redbooks Collection	
Networking and Systems Management Redbooks Collection	SK2T-2177
Transaction Processing and Data Management Redbook	SK2T-6022
AS/400 Redbooks Collection	SK2T-8038
RS/6000 Redbooks Collection (HTML, BkMgr)	SK2T-2849
RS/6000 Redbooks Collection (PostScript)	SK2T-8040
Application Development Redbooks Collection	SK2T-8041
Personal Systems Redbooks Collection	SK2T-8037
	SK2T-8042

# Related Publications - Continued



## Other Publications

- *These publications are also relevant as further information sources:*

IBM Redbooks: <http://www.redbooks.ibm.com>

AS/400 Information Center: <http://www.as400.ibm.com/infocenter>

Title	Publication Number
<i>AS/400 Internet Security: Implementing AS/400 VPNs</i>	SG24-5404-00
<i>A Comprehensive Guide Virtual Private Networks, Volume I: IBM Firewall, Server Client Solutions</i>	SG24-5201-00
<i>A Comprehensive Guide Virtual Private Networks, Volume II: IBM Nways Router Solutions</i>	SG24-5234-01
<i>A Comprehensive Guide Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management</i>	SG24-5309-00
<i>IBM Firewall for AS/400 V4R3: VPN and NAT Support</i>	SG24-5376-00
<i>TCP/IP Tutorial and Technical Overview</i>	GG24-3376-05